Kommittémotion

Motion till riksdagen 2017/18:2343

av Stig Henriksson m.fl. (V)

Informations- och cybersäkerhet inom staten

1 Förslag till riksdagsbeslut

1. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör ta fram riktlinjer för hur outsourcing av it-verksamhet så långt det är möjligt ska kunna undvikas i den statliga förvaltningen och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör återkomma med ett förslag om statlig molntjänst i enlighet med Statens servicecenters rapport En gemensam statlig molntjänst för myndigheternas it-drift, (2017, R:001) och tillkännager detta för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen under mandatperioden bör återkomma med en strategi för statens informations- och cybersäkerhet utifrån SOU 2015:23 och tillkännager detta för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör fastställa en tidsplan för när målen i strategin ska vara uppfyllda och överväga sanktionsmöjligheter för de myndigheter som inte uppfyller godtagbara krav på informations- och cybersäkerhet, och detta tillkännager riksdagen för regeringen.

2 Allvarliga brister i myndigheternas informationssäkerhetsarbete

Statsförvaltningen hanterar dagligen mängder av information. Mycket av det som skapas och lagras är både viktigt och känsligt. Vissa uppgifter klassas som skyddsvärda och en del rör även rikets säkerhet. Om informationen går förlorad, stjäls, manipuleras eller sprids till obehöriga kan det få allvarliga följder. Konsekvenserna kan t.ex. vara att integritetskänsliga uppgifter sprids, betalningar uteblir, el- eller vattenförsörjningen störs eller att uppgifter om samhällsviktiga funktioner kommer obehöriga till del. Informationssäkerhet handlar om att all skyddsvärd information är tillgänglig, riktig, konfidentiell och spårbar.

Riksrevisionen har återkommande granskat myndigheternas informationssäkerhetsarbete. Tidigare rapporter har visat på ett flertal brister. Bl.a. har

myndigheternas förutsättningar för ett effektivt informationssäkerhetsarbete liksom uppföljningsarbetet varit alltför dåligt.

Den senaste rapporten (RiR 2016:8) visar på liknande problem. Nivån på informationssäkerheten hos de granskade myndigheterna ligger märkbart under vad som är tillräckligt. En viktig förklaring är enligt Riksrevisionen att förståelsen för vikten av en god informationssäkerhet överlag är alltför liten. Det får i sin tur till följd att arbetet inte prioriteras tillräckligt i förhållande till riskerna. Riksrevisionen konstaterar vidare att regeringen inte har sett till att det finns nödvändiga förutsättningar för myndigheterna. Också Säpo har tidigare riktat kritik mot bristande it- och informationssäkerhet hos myndigheterna.

Samtidigt som myndigheterna inte klarar av att hantera uppgifterna är det dominerande påbudet att allt fler it-områden ska läggas ut på entreprenad. I Riksrevisionens rapport It i statsförvaltningen från 2011 kritiseras svenska myndigheter för att inte i tillräckligt hög utsträckning pröva frågan om outsourcing av it-verksamheten. Den dåvarande borgerliga regeringen gjorde sin hållning klar när man i efterföljande skrivelse slog fast att det är ”önskvärt att en större del av myndigheternas it-behov tillfredsställs med hjälp av outsourcing”.

Sammanfattningsvis har informationssäkerhetsarbetet inom staten under lång tid varit alltför dåligt. Att Riksrevisionen konstaterar att arbetet med informationssäkerhet inte når upp till en godtagbar nivå är allvarligt, liksom att regeringen inte har försäkrat sig om att det finns nödvändiga förutsättningar för myndigheterna att upprätthålla en god nivå. Det innebär att problemet är omfattande och att den enskilda myndigheten i sig inte har tillräckliga verktyg för att komma till rätta med de problem som finns. I stället har man lagt ut en allt större andel av it-verksamheten på externa aktörer, vilket i flera nyligen uppmärksammade fall fått stora negativa konsekvenser.

2.1 Transportstyrelsekrisen

I somras avslöjades en felaktig hantering av skyddsvärda uppgifter inom Transportstyrelsen. Sedan myndighetens start 2009 har Transportsstyrelsens it-tjänster hanterats av Trafikverket. År 2014 beslutade man att avbryta samarbetet med Trafikverket och i stället outsourca verksamheten. Upphandlingen vanns året därpå av it-företaget IBM som tog över driften av it-tjänsterna. Uppgifter i media gör gällande att avtalen var värda drygt 700 miljoner kronor och därmed en av de största affärerna i sitt slag som gjorts av en svensk myndighet.

Redan i maj 2015 uppdagades dock en rad problem gällande säkerhetsgranskningen av berörda tekniker hos IBM. För att skynda på processen och undvika att Transportstyrelsens register tillfälligt skulle behöva stängas ned beslutade dåvarande generaldirektör Maria Ågren att göra avsteg från såväl säkerhetsskyddslagen, personuppgiftslagen och offentlighets- och sekretesslagen som från myndighetens egna krav på informationssäkerhet. Detta ledde i sin tur till att känsliga uppgifter om b.la. skyddade identiteter, viss information gällande militära fordon och sårbar infrastruktur blev tillgängliga för IBM:s underleverantörer i både Tjeckien, Rumänien och Serbien och därmed för personal som inte genomgått någon säkerhetsgranskning. Upphandlingen skedde trots uppmaningar från både Säpo och Transportstyrelsens internrevisor om att avbryta affären.

Riksrevisionens rapport slår fast att sekretess och känsliga uppgifter kan vara skäl för att inte outsourca it-verksamheten hos en myndighet. Man poängterar också att det

visserligen kan vara möjligt att bibehålla en hög informationssäkerhet vid en outsourcing, men att ”det förutsätter en noggrann analys och god kravställning”, vilket tycks ha saknats i Transportstyrelsens upphandling.

Transportstyrelsens uppmärksammade upphandling föranleder en rad frågor som rör information och ansvar. Det är uppenbart att hanteringen av känsliga uppgifter har skötts illa och att viktiga säkerhetsfrågor har frångåtts. Därför är det nödvändigt och välkommet att ansvarsfrågan utreds så att de brister som funnits i regeringens hantering klargörs.

Ansvaret delas dock i hög grad av den förra borgerliga regeringen. Det är tydligt att upphandlingen i fråga inte hanterats på ett sätt som säkerställer att tillräckliga säkerhetshänsyn har tagits. Frågan är dock om en upphandling av det här slaget alls är lämplig. Trots detta gav den tidigare regeringen tydligt uttryck för att en större del av myndigheternas it-verksamhet skulle outsourcas. Det betyder i praktiken att privatisera verksamhet och det var en del i den borgerliga regeringens övergripande strategi för privatisering. Detta uttrycktes dock utan att tillhandahålla tillräckliga riktlinjer eller kriterier. Någonting som i Transportstyrelsens fall medfört mycket allvarliga konsekvenser. Inte heller skedde en tillräcklig utbildning vad gäller säkerhetsfrågor för de inblandade i upphandlingen.

Strax efter att problemen på Transportstyrelsen uppdagats gick media ut med uppgifter om att ännu en myndighet brustit i hanteringen när det gäller outsourcing av it-system. Denna gång gällde det Polismyndighetens lönesystem Palasso. Uppgifter gör gällande att Rikspolischef Dan Eliasson ska ha valt att göra avsteg från säkerhetsskyddsförordningen och gett sitt godkännande till att inte använda sig av Försvarsmaktskrypto utan att ansöka om dispens från regeringen. Detta har kritiserats hårt av bl.a. Militära underrättelse- och säkerhetstjänsten (MUST). I dagsläget råder det fortfarande oklarhet kring förfarandet och huruvida detta varit ett tillåtet avsteg eller inte. Att en sådan osäkerhet kring skyddsvärda uppgifter tillåts råda inom myndigheterna är allvarligt. För att en god informationssäkerhet ska kunna garanteras krävs tydliga och transparenta strukturer där sådana här oklarheter inte ska kunna uppstå.

Regeringen har med anledning av Transportstyrelsekrisen tillsatt en utredare som ska genomlysa händelserna som ledde fram till att säkerhetskänslig och av andra skäl sekretessbelagd information hanterades på ett sätt som strider mot svensk lagstiftning. Dessutom har man gett Transportstyrelsen själva i uppgift att kartlägga vilken information som har hanterats på ett felaktigt sätt och bedöma vilka åtgärder som eventuellt krävs för att hanteringen av skyddsvärda uppgifter framöver ska ske på ett lämpligt sätt. Vänsterpartiet menar att Transportstyrelsens hantering av information måste följas upp. Det är dock viktigt att se händelserna i ett större sammanhang. Riksrevisionens senaste granskning omfattade nio myndigheter, men man påpekar också att det inte finns någon anledning att tro att situationen skiljer sig från övriga myndigheter. Dessutom bottnar problemen i att regeringen inte har tagit tillräckligt ansvar för att säkerställa att myndigheterna har tillräckliga förutsättningar för ett gott informations- och cybersäkerhetsarbete. Problemet med bristande it-säkerhet är större än att enbart röra ett fåtal myndigheter.

3 Hot och risker

Både individer och samhällsstrukturen kräver stora mängder av information för att vardagen ska fungera. Dagens informationshantering sker i hög utsträckning med hjälp av olika it-system. En hög it-användning leder ofta till effektivisering och mer välfungerande tjänster och verksamheter, men innebär även digitala säkerhetsrisker. Det har också skett en tydlig ökning av incidenter relaterade till internet, såsom dataintrång, bedrägerier och spridning av skadlig kod. Vem som ligger bakom kan variera, men det kan t.ex. både handla om privatpersoner, organiserad brottslighet, terrorister och andra statsmakter. Spridning av skyddsvärd information kan både ske p.g.a. slarv eller obetänksamhet, eller genom att någon aktivt ser till att skaffa sig den.

En bristande informationssäkerhet riskerar att få förödande konsekvenser. Incidenter eller störningar som angriper den digitala infrastrukturen kan leda till omfattande problem för t.ex. de finansiella systemen, hälso- och sjukvården, livsmedelsförsörjningen eller den nationella säkerheten. När hanteringen av viktig information brister riskerar detta också att leda till ett försämrat förtroende för etablerade samhällsstrukturer.

En politisk vilja till ökad outsourcing av it-tjänster måste sättas i relation till vilka säkerhetsrisker det kan medföra. I fallet med Transportstyrelsen framkom först i efterhand att man inte kunde kräva någon säkerhetsgranskning av de anställda som skulle hantera systemen. När kortsiktig vinst blir en drivkraft för att upprätthålla fungerande it-system sätts långsiktigheten på undantag och helheten går förlorad. Outsourcing av skyddsvärda uppgifter bör endast ske i undantagsfall. Regeringen bör ta fram riktlinjer för hur outsourcing av it-verksamhet så långt det är möjligt ska kunna undvikas i den statliga förvaltningen. Detta bör riksdagen ställa sig bakom och ge regeringen till känna.

Att skyddsvärd information skulle komma obehöriga till del kan innebära en nationell säkerhetsrisk, men också ett enskilt hot mot de individer som eventuellt drabbas. Att hemliga identiteter offentliggörs, att journalisters källor hängs ut eller att uppgifter om vem som arbetar på viktiga nyckeltjänster inom t.ex. Polisen blir tillgängliga undergräver i förlängningen det demokratiska samhället. Den offentliga förvaltningen kräver en nödvändig tillit mellan medborgare och stat. Myndigheter som samverkar måste våga göra det utan att uppleva att informationen hanteras på ett otillfredsställande sätt.

Sverige och världen står i dag inför större utmaningar än på länge och vi befinner oss i ett i många avseenden nytt säkerhetspolitiskt läge. Utgångspunkten för Sveriges försvars- och säkerhetspolitik ska vara att värna vårt lands säkerhet. Det kräver en modern försvarsmakt som har förmågan att möta de olika former av hot som vårt land kan ställas inför. Ett framgångsrikt totalförsvar kräver dock att samhället i övrigt är robust och upprätthåller en hög nivå av säkerhet inom de samhällsviktiga strukturerna. Där utgör informations- och cybersäkerhet ett särskilt viktigt område.

I dag bygger en stor del av den svenska krisberedskapen på att vi har fungerande it-system för t.ex. logistik och försörjning av el och vatten. Vid ett haveri riskerar viktiga samhällsfunktioner att drabbas hårt eller rent av slås ut. Ett tryggt och robust system måste utgå från välgrundade och motiverade riskbedömningar. Det kräver både att det finns tillräcklig kunskap och kompetens och att arbetet sker regelbundet och systematiskt med återkommande uppföljning.

Det pågår just nu ett arbete med att implementera det s.k. NIS-direktivet (The Directive on security of network and information systems) i svensk rätt. Direktivet handlar om åtgärder för en hög gemensam nivå på säkerhet i närverks- och informationssystem i EU, (EU 2016/1148). Det innebär bl.a. skyldigheter för vissa leverantörer av samhällsviktiga tjänster och vissa leverantörer av digitala tjänster att vidta säkerhetsåtgärder för att hantera risker samt förebygga och hantera incidenter i nätverk och informationssystem. Ett antal myndigheter föreslås vara tillsynsmyndigheter för de olika samhällssektorerna. Frågan är dock hur väl tillsynen kommer att fungera om inte myndigheterna själva klarar sitt eget säkerhetsarbete.

4 Vikten av fungerande strukturer

Ett av de allvarligaste påpekandena från Riksrevisionen rör regeringens bristande arbete för att möjliggöra ett gott informationssäkerhetsarbete inom myndigheterna. Det är tydligt att det krävs ett omfattande arbete för att skapa reella förutsättningar för myndigheterna att arbeta med detta.

Våren 2017 presenterade Statens servicecenter rapporten En gemensam statlig molntjänst för myndigheternas it-drift, (R:001). Rapporten föreslår att myndigheternas it-drift samordnas i en statlig molntjänst. I dag ansvarar varje statlig myndighet för sin egen it-drift och myndigheternas it-verksamhet är spridd över ett stort antal datacenter, varav de flesta är koncentrerade till Stockholm. Dagens system är kostsamt och uppnår inte alltid de säkerhets- och integritetskrav man rimligen bör kunna ställa på den offentliga förvaltningen. Rent konkret föreslår Statens servicecenter att myndigheternas datalagring i framtiden i stället sker genom en gemensam molntjänst som är uppbyggd på tio olika datacenter i bergrum utanför storstadsområdena. Enligt rapporten skulle myndigheterna kunna spara 30 procent av dagens it-kostnader med en sådan molnlösning och systemet skulle bli väsentligt mycket säkrare än i dag. Regeringen bör därför återkomma med ett förslag om statlig molntjänst i enlighet med Statens servicecenters rapport En gemensam statlig molntjänst för myndigheternas it-drift, (2017, R:001). Detta bör riksdagen ställa sig bakom och ge regeringen till känna.

I mars 2015 lämnade informationssäkerhetsutredningen (NISU 2014) över sitt betänkande Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten (SOU 2015:23). Utredningen föreslår en strategi med sex mål: att stärka styrning och tillsyn inom området, att staten ska ställa tydliga krav vid upphandling på it-området, att statliga myndigheter ska kommunicera säkert, att det ska inrättas ett system för obligatorisk it-incidentrapportering för samtliga statliga myndigheter, att arbetet med att förebygga och bekämpa it-brottslighet ska stärkas samt att Sverige ska vara en stark internationell partner.

Vänsterpartiet menar att det är av stor vikt att brådskande stärka arbetet för ökad informations- och cybersäkerhet. För ett gemensamt förhållningssätt inom staten krävs en tydligare samordning på initiativ från regeringen. Utredningen föreslår en rad viktiga målsättningar som bör ligga till grund för det fortsatta arbetet. Men trots att det var över två år sedan utredningen presenterade sitt betänkande har mycket lite hänt. Med tanke på den allvarliga kritik som framförts från bl.a. Riksrevisionen bör tempot höjas i arbetet med att skydda samhällsviktiga funktioner och system. Regeringen bör under

mandatperioden återkomma med en strategi för statens informations- och cybersäkerhet utifrån SOU 2015:23. Detta bör riksdagen ställa sig bakom och ge regeringen till känna.

Regeringen bör även fastställa en tidsplan för när målen i strategin ska vara uppfyllda samt överväga sanktionsmöjligheter för de myndigheter som inte uppfyller godtagbara krav på informations- och cybersäkerhet. Detta bör riksdagen ställa sig bakom och ge regeringen till känna.

Stig Henriksson (V)

Jens Holm (V)

Amineh Kakabaveh (V)

Birger Lahti (V)

Yasmine Posio Nilsson (V)

Håkan Svenneling (V)

Emma Wallrup (V)