Enskild motion

Motion till riksdagen 2017/18:226

av Daniel Bäckström (C)

med anledning av skr. 2016/17:213 Nationell strategi för samhällets informations- och cybersäkerhet

Förslag till riksdagsbeslut

1. Riksdagen ställer sig bakom det som anförs i motionen om att se över om de befintliga regelverk som styr kommunernas krav på informations- och cybersäkerhet, inklusive tillsyn, är tillräckliga eller behöver tydliggöras, och detta tillkännager riksdagen för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om att strategin behöver kompletteras med ambitioner och förslag för att motverka den ökade trenden med cyberbaserat industriellt ekonomiskt spionage, och detta tillkännager riksdagen för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om att åtgärder behöver vidtas för att säkra it-hanteringen och stärka it- och cybersäkerheten generellt men inte minst för de verksamheter, privata och offentliga, som äger och driver samhällsviktig verksamhet eller infrastruktur eller i övrigt hanterar frågor som rör rikets säkerhet, och detta tillkännager riksdagen för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om att ta fram strategier för ett generellt kompetenslyft avseende informations- och cybersäkerhet och säkerhetsskydd och tillkännager detta för regeringen.
5. Riksdagen ställer sig bakom det som anförs i motionen om att EU bör få en större och tydligare roll vad gäller cybersäkerhet, och detta tillkännager riksdagen för regeringen.

Motivering

En god informations- och cybersäkerhet är mycket viktigt. Flera rapporter de senaste åren, exempelvis Riksrevisionens genomgång av informationssäkerheten hos nio myndigheter såväl som Myndigheten för samhällsskydd och beredskaps (MSB) nationella risk- och förmågebedömning, visar att samhällets arbete med informations-

och cybersäkerhet behöver utvecklas ordentligt. Det är allvarligt att bristerna är så stora. Inte minst sommarens händelser med Transportstyrelsens beslut att göra avsteg från säkerhetsskyddslagstiftningen visar att säkerhetsarbete generellt och informations- och cybersäkerhet specifikt behöver uppgraderas och i större avseende än hittills beaktas i beslutsfattande och verksamhetsutveckling. Det här är också en trend som bl.a. Försvarets radioanstalt (FRA) har identifierat, och de beskriver att ”… säkerheten hos myndigheter och statliga bolag inte är dimensionerad för den hotbild vi ser”.[1] En skrivelse med namnet Nationell strategi för samhällets information och cybersäkerhet ger förhoppningar om en heltäckande strategi som tar ett brett grepp om samhällets information och cybersäkerhet, men tyvärr levererar regeringen många fina ord, ibland rena plattityder, med liten konkretion.

Regeringen föreslår en nationell modell för systematisk informationshantering, vilket ter sig lovvärt och i flera avseenden säkerligen skulle underlätta för aktörer att arbeta med informations- och cybersäkerhet. Det är bra, även om det inte är säkert att en modell passar alla aktörer beroende på deras olika uppdrag, storlek, ansvarsområden osv. Det riskerar i värsta fall att bli ett stelbent verktyg. Varför modellen i ett första skede endast ska inrikta sig på statliga myndigheter är också oklart, inte minst eftersom bristerna på kommunal nivå också är stora. Om modellen kan tydliggöra och stödja aktörer, privata och offentliga, att ställa krav på säkerhet är det bra. I regeringens skrivelse framkommer dock inte vilken status modellen ska ha, varför den riskerar att bli verkningslös. Det framkommer inte heller vad som sker om aktörerna inte använder sig av den. Frågan om tillsyn tas upp i strategin, vilket är bra, men kan behöva kopplas även till det systematiska cyber- och informationssäkerhetsarbetet.

Minst lika viktigt som en nationell modell är att det finns tydlig styrning, lagar och regler som gör att aktörer måste beakta, ta hänsyn till och arbeta med systematisk informationssäkerhet i sin verksamhet. Skrivelsen tycks i huvudsak vara inriktad på statliga myndigheter, och ofta saknas resonemang om hur statsmaktens regelstyrning avseende informationssäkerhet kan tydliggöras för aktörer som inte är statliga myndigheter. Inte minst MSB har visat att det systematiska informationssäkerhetsarbetet ofta brister också på kommunal nivå.[2] Perspektivet att styrningen i förhållande till de statliga myndigheterna ska tydliggöras är därför inte tillräckligt brett för att främja hela samhällets systematiska informationssäkerhetsarbete. Det är uppenbart att dagens regelverk inte varit tillräckligt för att få exempelvis kommuner att arbeta systematiskt med informationssäkerhet. Regeringen bör därför, utöver en nationell modell, se över om regelstyrningen och kraven på cyber- och informationssäkerhet i förhållande till inte minst kommunerna är tillräcklig. Här bör också möjligheten för MSB att få föreskriftsrätt i förhållande till kommunernas systematiska informationssäkerhetsarbete prövas. Därtill bör i en sådan översyn beaktas ett eventuellt behov av ökad tillsyn på området.

Regeringen tar viktiga steg i den nationella strategin för samhällets informations- och cybersäkerhet men når inte riktigt ända fram för att skrivelsen ska göra skäl för sitt namn. Det brottsförebyggande perspektivet finns med men det saknas ambitioner och konkreta förslag för att motverka den ökande trenden av cyberbaserat industriellt ekonomiskt spionage. FRA har identifierat att statsunderstödda cyberaktiviteter mot

[1] FRA årsrapport 2016.

[2] https://www.informationssakerhet.se/rapportsida/en-bild-av-kommunernas-informationssakerhetsarbete-20151/.

Sverige inte enbart riktar sig mot föremål som strikt befinner sig inom ramen för nationell säkerhet (försvar m.m.) utan även är riktade mot industrin, forskningen samt kritisk infrastruktur. Det är därför viktigt att strategin kompletteras med tydliga ambitioner och konkreta förslag för att motverka och hantera också denna typ av cyber-spionage.

När det gäller säkra kryptolösningar konstaterar regeringen i skrivelsen att ”Sverige behöver tillgång till teknisk kompetens inom kryptoområdet för att säkerställa nödvändigt signalskydd, såväl för den ordinarie verksamheten som vid tillfällen då samhället utsätts för påfrestningar”, men tyvärr presenteras inga förslag på hur denna tekniska specifika kompetens ska säkerställas. Centerpartiet vill här understryka vikten av att informationssäkerhet, inklusive krypto, inte enkom ses som en teknisk fråga som kräver teknisk kompetens. För ett framgångsrikt informationssäkerhetsarbete krävs förståelse för frågan i en organisations alla funktioner. Jurister, analytiker, ekonomer, upphandlingsexpertis, registratur m.fl. behöver alla ha kunskap om och kunna förhålla sig till vad som är skyddsvärd information. Ett generellt kunskapslyft om informationssäkerhet och säkerhetsskydd behövs inom de flesta organisationer. Regeringen lyfter fram forskning och högre utbildning inom informationssäkerhetsområdet, vilket är bra, men långt ifrån tillräckligt. Än en gång saknas en helhetssyn i nationella strategin. Det hade varit önskvärt om regeringen också kommit med förslag på *hur* en generell kunskapshöjning kan ske. Finns det ingen förståelse för vikten av systematiskt informationssäkerhetsarbete hos allt från en organisations registratur och vaktmästeri till högsta ledning ökar risken för brister i informationssäkerhetsarbetet. Hur enskilda förhåller sig till säkerheten kring information är ytterst viktigt för att kunna upprätthålla ett gott skydd, men det är tveksamt om de insatser som bedrivs av ett fåtal myndigheter i dag för öka individers kunskap verkligen är tillräckliga. Högre ambitioner behövs.

Centerpartiet hade gärna sett utvecklade resonemang kring informationssäkerhet som ett förhållningssätt i organisationer som arbetar med krisberedskap och totalförsvarsplanering. När totalförsvarsplaneringen nu intensifieras finns i många organisationer ett behov av att kunna skydda information som inte är elektronisk eller digitaliserad; det handlar om att den kan vara så skyddsvärd att elektroniska verktyg inte alls ska användas, eller endast krypteringsverktyg användas. I dag saknas på många ställen möjligheter att tala om hemligheter i skyddade lokaler. Det hade varit bra om svar kring hur denna problematik ska lösas hade funnits i strategin. Det är oklart om det i alla relevanta organisationer finns tillräcklig kunskap om vad som är hemlig information, eller hur den måste hanteras. Även här krävs ett allmänt kunskapslyft. Åtgärder behöver vidtas för att säkra it-hanteringen och stärka it- och cybersäkerheten generellt men inte minst för de verksamheter, privata och offentliga, som äger och driver samhällsviktig verksamhet, infrastruktur eller i övrigt hanterar frågor som rör rikets säkerhet. Funktionskrav på samhällsviktig verksamhet behöver tas fram.

Frågan om säkerhet och integritet tas upp i skrivelsen, vilket är bra. Frågor kring privatliv och integritet aktualiseras när information om individer finns i allt fler digitala system, som kanske inte alltid har ett fullgott skydd. Det är en stor och potentiell säkerhetsrisk som måste beaktas och hanteras.

Vikten av att delta i internationella samarbeten för att öka den nationella förmågan att hantera cyberhot lyfts i skrivelsen. Centerpartiet hade gärna sett tydligare resonemang och förslag om hur regeringen vill att EU ska utvecklas på cyberområdet. För Centerpartiet vill att EU ska få en större roll i frågor kring informations- och

cybersäkerhet. Inget system är starkare än sin svagaste länk, och inom Europa är många system sammanlänkade. Nätverks- och informationssystem, och internet i synnerhet, spelar en viktig roll för rörligheten för varor, tjänster och personer inom EU. Eftersom så mycket är sammanlänkat kan också små avbrott snabbt bli stora och påverka inte bara enskilda människor i vardagen utan också enskilda länder och unionen som helhet. Att EU:s samlade förmåga på området stärks är därför av vikt. Centerpartiet vill att minimikraven för informationssäkerhet i alla EU:s medlemsländer höjs.

Effektiva åtgärder för att förstärka säkerheten i nätverks- och informationssystemen förutsätter åtgärder på EU-nivå. Även i det operativa arbetet med att hantera cyberkriser kan det finnas anledning att stärka det europeiska samarbetet.

Daniel Bäckström (C)