Försvarsutskottets betänkande
2023/24:FöU2

Riksrevisionens rapport om regeringens styrning av samhällets informations- och cybersäkerhet

Sammanfattning

Utskottet föreslår att riksdagen lägger skrivelsen till handlingarna och avslår samtliga motionsyrkanden, i huvudsak med hänvisning till redan pågående arbeten.

I skrivelsen redogör regeringen för sin bedömning av de slutsatser och rekommendationer som Riksrevisionen lämnar i rapporten Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig.

Riksrevisionens övergripande slutsats är att regeringens arbete inom området inte har varit effektivt utformat. Enligt Riksrevisionen handlar den centrala bristen om avsaknad av strategiska avvägningar och prioriteringar som inriktar informations- och cybersäkerhetsarbetet.

Regeringen välkomnar granskningen och instämmer huvudsakligen i Riksrevisionens iakttagelser. Regeringen kommer därför att överväga hur den nya nationella informations- och cybersäkerhetsstrategin bör utformas för att hantera de brister som iakttagits.

Regeringen delar Riksrevisionens bedömning att det har tagit lång tid att bygga upp det nationella cybersäkerhetscentret (NCSC) och att ansvarsfördelningen inom centret gör verksamheten svår att styra och följa upp. Försvarsdepartementet har därför gett en utredare i uppdrag att lämna förslag på hur Försvarets radioanstalt (FRA) ska tilldelas huvudansvaret för NCSC. Utredaren ska också se över centrets organisation och styrning.

I och med denna skrivelse anser regeringen att Riksrevisionens rapport är slutbehandlad.

I betänkandet finns tio reservationer (S, V, C, MP).

Behandlade förslag

Skrivelse 2023/24:26 Riksrevisionens rapport om regeringens styrning av samhällets informations- och cybersäkerhet.
Två yrkanden i en följdmotion.
20 yrkanden i motioner från allmänna motionstiden 2023/24.

Innehållsförteckning

Utskottets förslag till riksdagsbeslut

1. Stärkt förmåga

Riksdagen avslår motionerna
2023/24:415 av Jimmy Ståhl m.fl. (SD) yrkande 7,
2023/24:1903 av Peter Hedberg och Malin Larsson (båda S),
2023/24:2450 av Emma Berginger m.fl. (MP) yrkande 5 och
2023/24:2564 av Peter Hultqvist m.fl. (S) yrkande 60.

Reservation 1 (S)
Reservation 2 (MP)

2. Det nationella cybersäkerhetscentret

Riksdagen avslår motionerna
2023/24:422 av Tobias Andersson m.fl. (SD) yrkande 3 och
2023/24:2765 av Mikael Larsson och Niels Paarup-Petersen (båda C) yrkandena 1 och 2.

Reservation 3 (C)

3. It-haverikommission

Riksdagen avslår motion
2023/24:461 av Hanna Gunnarsson m.fl. (V) yrkande 4.

Reservation 4 (V)

4. Kunskapsuppbyggnad

Riksdagen avslår motionerna
2023/24:422 av Tobias Andersson m.fl. (SD) yrkandena 4 och 7,
2023/24:497 av Rashid Farivar m.fl. (SD) yrkande 12,
2023/24:880 av Markus Wiechel och Björn Söder (båda SD),
2023/24:2450 av Emma Berginger m.fl. (MP) yrkande 7 och
2023/24:2564 av Peter Hultqvist m.fl. (S) yrkande 59.

Reservation 5 (S)
Reservation 6 (MP)

5. Samverkan

Riksdagen avslår motion
2023/24:422 av Tobias Andersson m.fl. (SD) yrkandena 5 och 6.

6. Outsourcing och upphandling

Riksdagen avslår motionerna
2023/24:415 av Jimmy Ståhl m.fl. (SD) yrkande 6 och
2023/24:461 av Hanna Gunnarsson m.fl. (V) yrkandena 2 och 3.

Reservation 7 (V)

7. Molntjänster

Riksdagen avslår motionerna
2023/24:461 av Hanna Gunnarsson m.fl. (V) yrkande 6 och
2023/24:2564 av Peter Hultqvist m.fl. (S) yrkande 17.

Reservation 8 (S)
Reservation 9 (V)

8. Internationellt regelverk

Riksdagen avslår motion
2023/24:461 av Hanna Gunnarsson m.fl. (V) yrkande 1.

Reservation 10 (V)

9. Skrivelsen

Riksdagen lägger skrivelse 2023/24:26 till handlingarna.

Stockholm den 14 december 2023

På försvarsutskottets vägnar

Peter Hultqvist

Följande ledamöter har deltagit i beslutet: Peter Hultqvist (S), Lars Wistedt (SD), Jörgen Berglund (M), Björn Söder (SD), Johan Andersson (S), Anna Starbrink (L), Erik Ezelius (S), Alexandra Anstrell (M), Hanna Gunnarsson (V), Mikael Oscarsson (KD), Mikael Larsson (C), Lars Püss (M), Emma Berginger (MP), Gustaf Göthberg (M), Markus Selin (S), Camilla Brunsberg (M) och Lena Johansson (S).

Redogörelse för ärendet

Ärendet och dess beredning

Riksrevisionen har granskat regeringens styrning av samhällets informations- och cybersäkerhet (RiR 2023:8). Riksdagen överlämnade Riksrevisionens rapport till regeringen den 24 april 2023. I den skrivelse som försvarsutskottet här bereder behandlar regeringen de iakttagelser och rekommendationer som Riksrevisionen redovisar i sin rapport. Två yrkanden i en följdmotion samt 20 yrkanden i motioner från allmänna motionstiden 2023/24 behandlas i betänkandet.

Riksrevisor Helena Lindberg med medarbetare lämnade den 30 november 2023 information i utskottet om Riksrevisionens granskningsrapport.

Bakgrund

Riksrevisionen har mot bakgrund av de utmaningar som finns på informations- och cybersäkerhetsområdet undersökt hur regeringen arbetar för att stärka Sveriges informations- och cybersäkerhet. Riksrevisionen har granskat om den nationella informations- och cybersäkerhetsstrategin är effektivt utformad samt om regeringen genomfört den nationella informations- och cybersäkerhetsstrategin på ett effektivt sätt.

Utskottets överväganden

Regeringens styrning av samhällets informations- och cybersäkerhet

Utskottets förslag i korthet

Riksdagen lägger skrivelsen till handlingarna och avslår samtliga motionsyrkanden, i huvudsak med hänvisning till redan pågående arbeten.

Jämför reservation 1 (S), 2 (MP), 3 (C), 4 (V), 5 (S), 6 (MP), 7 (V), 8 (S), 9 (V) och 10 (V).

Riksrevisionens iakttagelser och rekommendationer

Riksrevisionens samlade slutsats är att regeringens arbete för att stärka Sveriges informations- och cybersäkerhet inte har varit effektivt. Riksrevisionen anser att regeringens strategi och genomförandet av den inte når upp till vad som anses vara internationell bästa praxis, som i huvudsak baseras på Europeiska unionens cybersäkerhetsbyrås (European Union Agency for Network and Information Security) s.k. Good Practice Guide. Enligt Riksrevisionen är den centrala bristen att det saknas strategiska avvägningar och prioriteringar som borde rikta in arbetet. Bristerna i strategin och dess genomförande grundar sig, enligt Riksrevisionen, i Regeringskansliets organisation och arbetsmetoder. Riksrevisionen anser att Regeringskansliets arbetsmetoder, organisering och resursanvändning inte har möjliggjort ett effektivt arbete med informations- och cybersäkerhetsfrågorna.

Enligt Riksrevisionen visar granskningen att det har funnits svårigheter i att säkerställa en effektiv samordning som involverar relevanta intressenter, vilket skapat en svag styrning från regeringens sida. Riksrevisionens bedömning är att regeringens arbete på området inte har lett till en ökad förmåga att prioritera insatser utifrån Sveriges samlade behov av informations- och cybersäkerhet eller till en långsiktig, strategisk, holistisk och sammanhållen styrning av informations- och cybersäkerhetsområdet.

Riksrevisionen bedömer att det bl.a. saknas tillräcklig operativ och taktisk kunskap i Regeringskansliet om hur cybersäkerhetsarbetet bedrivs på myndigheterna och inom den privata sektorn. Riksrevisionen konstaterar också att en strategi som inte pekar ut ansvar eller resurser innebär låg eller ingen styreffekt.

Granskningsrapporten visar att styrningen av enskilda myndigheter i huvudsak har varit tydlig och att finansiella resurser har tilldelats myndigheter i vissa fall. Riksrevisionen konstaterar däremot att de flesta åtgärderna ska

genomföras inom befintliga anslag och att strategin inte pekar ut ansvariga för att genomföra åtgärder inom de prioriterade områdena.

Riksrevisionen bedömer att en svag styrning lett till att regeringens ambitioner på informations- och cyberssäkerhetsområdet inte har infriats och att regeringen inte har agerat tillräckligt i flera centrala frågor. Det konstateras bl.a. att regeringen inte har vidtagit åtgärder när relevanta myndigheter inte nått samsyn i arbetet med att ta fram en gemensam nationell modell för informations- och cybersäkerhet inom ramen för Samverkansgruppen för informationssäkerhet och Nationellt cybersäkerhetscenter (NCSC).

I sammanhanget konstaterar Riksrevisionen att det har tagit lång tid att bygga upp NCSC. Orsaken till detta förklaras ligga i att mycket tid har gått åt till att lösa frågor kring formerna för samverkan och att ansvaret för frågor som krävt insatser från flera olika aktörer, eller frågor som inte tillhör någon aktörs huvudprioriteringar, till viss del har varit otydligt. Riksrevisionen konstaterar också att privata aktörer har involverats i begränsad omfattning, både när det gäller framtagandet av strategin och uppbyggnaden av NCSC.

Enligt Riksrevisionen visar granskningen att det har skapats en fragmenterad bild av området på grund av att myndigheterna i dagsläget tar fram flera olika lägesbilder. Riksrevisionen bedömer att detta har försvårat möjligheten att väga olika åtgärder mot varandra och att det därför är viktigt att myndigheterna och regeringen identifierar vilka utmaningar som finns och hittar strukturer för att hantera dem.

Riksrevisionen anser att framsteg har gjorts hos en del aktörer under perioden då informations- och cybersäkerhetsstrategin varit på plats men konstaterar trots detta att det inte går att se någon generell förbättring av säkerheten, och därför kvarstår utmaningar inom strategins alla områden. Riksrevisionen konstaterar att det fortfarande finns problem med att utreda it-relaterade brott och att stötta olika aktörer vid incidenter trots att lagändringar har gjorts på området och att bristen på kompetens i samhället kopplat till informations- och cybersäkerhet är fortsatt kritisk.

Riksrevisionen konstaterar också att en stor del av Regeringskansliets resurser går åt till att hantera initiativ från EU utan att Sverige driver någon sammanhållen linje på EU-nivå.

Vidare visar granskningen att vissa aktörer inte upplever att de inkluderats på det sätt som de borde. Exempelvis framför aktörer inom näringslivet att de saknar stöd från statens sida.

Riksrevisionen lämnar följande rekommendationer till regeringen:

1. Skapa en strategisk, holistisk och långsiktig inriktning för arbetet med informations- och cybersäkerhet. Inriktningen bör omfatta en analys av de nationella strategiska utmaningarna, avvägningar och prioriteringar samt resurstilldelning och handlingsplan för genomförandet. Arbetet bör involvera berörda intressenter.

2. Säkerställ en samlad styrning med tydlig ansvarsfördelning, tillräcklig kompetens och effektiva former för samordning av informations- och cybersäkerhetsfrågorna i Regeringskansliet.
3. Identifiera hinder för informationsutbyte och se till att det finns strukturer som medger det informationsutbyte som är nödvändigt mellan myndigheter såväl som mellan det offentliga och det privata för att arbetet med samhällets informations- och cybersäkerhet ska fungera effektivt.
4. Se över det nationella informations- och cybersäkerhetscentrets uppdrag, mandat och organisatoriska hemvist för att säkerställa dess bidrag till hela samhällets informationssäkerhet såväl som cybersäkerhet.

Regeringens bedömning och åtgärder med anledning av Riksrevisionens iakttagelser

Riksrevisionens granskningsrapport tar sikte på den förra regeringens strategi för informations- och cybersäkerhet. Rapporten utgör ett värdefullt underlag för regeringens arbete med att ta fram en ny informations- och cybersäkerhetsstrategi. Riksrevisionens övergripande slutsats är att regeringens arbete för att stärka Sveriges informations- och cybersäkerhet inte har varit effektivt. Regeringen instämmer huvudsakligen i Riksrevisionens bedömning. Informations- och cybersäkerhetsområdet behöver vara mer strategiskt sammanhållet och det behöver finnas tydliga välgrundade prioriteringar som kan rikta in det dagliga arbetet för såväl Regeringskansliet, myndigheter och kommuner som näringsliv. Regeringen redogör i skrivelsen för sin bedömning av de iakttagelser som Riksrevisionen gör i sin rapport.

Riksrevisionen rekommenderar inledningsvis att det skapas en strategisk, holistisk och långsiktig inriktning för arbetet med informations-och cybersäkerhet. Regeringen håller med om Riksrevisionens bedömning och konstaterar att de iakttagelser som Riksrevisionen gör är värdefulla för den fortsatta utvecklingen av arbetet med informations- och cybersäkerhet.

Regeringen kommer att påbörja arbetet med att ta fram en ny informations- och cybersäkerhetsstrategi som ligger i linje med Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet). I det arbetet kommer regeringen att lägga vikt vid att analysera de nationella strategiska utmaningarna och att strategin harmonierar med andra eventuellt angränsande strategier. Stödet till och samverkan med statliga myndigheter och näringsliv är viktigt för regeringen och kommer att utgöra en central fråga när strategin tas fram.

Riksrevisionen konstaterar att Regeringskansliet saknar tillräcklig operativ och taktisk kunskap om hur cybersäkerhetsarbetet bedrivs inom både myndigheterna och den privata sektorn. Regeringen konstaterar att det, precis som med annan it-kompetens, råder brist på informations- och cybersäkerhetskompetens i samhället i stort och att behovet kommer att öka.

Det kommer att krävas breda och långsiktiga insatser i samhället för att komma till rätta med dessa utmaningar. EU-kommissionens förslag att lansera en akademi för cyberkompetens (Cyber Security Skills Academy) är en del i att åtgärda kompetensbristen inom cybersäkerhet vilket ska bidra till en ökad cyberresiliens inom EU.

Regeringen vill vidare understryka att Regeringskansliets uppgift är att bereda regeringsärenden och i övrigt biträda regeringen och statsråden i deras verksamhet. Stöd från expertmyndigheter inom området är avgörande. Försvarsdepartementet har dock fått utökade resurser och anställt flera medarbetare inom bl.a. informations- och cybersäkerhet. Det är statsministern som beslutar vilka statsråd som ska ingå i regeringen. Regeringskansliets organisation i olika departement bestäms av regeringen genom förordning.

Regeringen har flyttat ansvaret för samordning av civilt försvar och krisberedskap från Justitiedepartementet till Försvarsdepartementet och utsett en särskild minister för civilt försvar. Statsrådet för civilt försvar har, med stöd av förordnande enligt 7 kap. 5 § regeringsformen, bl.a. ansvar för förvaltningsärenden som gäller informations- och cybersäkerhet i den mån sådana ärenden inte hör till något annat departement. Dessa åtgärder kommer på sikt att skapa förutsättningar att ta ett samlat grepp om informations- och cybersäkerhetsfrågorna.

Regeringen har också inrättat ett nationellt säkerhetsråd för informationsutbyte och strategisk samordning i frågor som rör nationell säkerhet. För att biträda det nationella säkerhetsrådet har regeringen utsett en nationell säkerhetsrådgivare som ska svara för samordning, inriktning och analys av frågor som rör nationell säkerhet. Det är exempel på åtgärder som regeringen har vidtagit för att samordna och organisera Sveriges arbete med frågor om nationell säkerhet och krishantering så att det speglar dagens komplexa hotbild. Det nationella säkerhetsrådet ger möjlighet att lyfta fram frågor som behöver samordnas över departementsgränserna. Genom dessa åtgärder bedömer regeringen att det numera finns goda förutsättningar att uppnå en samlad styrning och effektiva former för samordning av informations- och cybersäkerhetsfrågorna.

Enligt Riksrevisionen har informationsutbytet mellan såväl myndigheter som mellan näringslivet och det offentliga inte fungerat väl. Riksrevisionen konstaterar att myndigheterna i dag tar fram flera olika lägesbilder och att det ger en fragmenterad bild av området som inte tillgodoser behovet av överblick. Regeringen instämmer i huvudsak med Riksrevisionens iakttagelse att informationsutbytet mellan näringslivet och det offentliga kan förbättras. Detta kommer att vara en viktig fråga att omhänderta i den nya informations- och cybersäkerhetsstrategin. Krav på utbyte av information mellan behöriga myndigheter följer också av NIS2-direktivet som det fattades beslut om i december 2022 och som ska genomföras i alla EU:s medlemsstater. Enligt direktivet ska myndigheter utbyta information med varandra om hot och incidenter samt om åtgärder som myndigheterna vidtar. I februari 2023 gav regeringen en särskild utredare i uppdrag att föreslå de anpassningar av svensk

rätt som behövs för att EU-direktivet ska kunna genomföras. Utredningen ska redovisa sitt uppdrag senast den 23 februari 2024. Ytterligare åtgärder när det gäller informationsutbyte är således att vänta med anledning av genomförandet av NIS2-direktivet.

Slutligen rekommenderar Riksrevisionen att regeringen ska se över det nationella informations- och cybersäkerhetscentrets uppdrag, mandat och organisatoriska hemvist. Den 10 december 2020 beslutade regeringen att ge FRA, Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB) och Säkerhetspolisen i uppdrag att fördjupa samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter, NCSC (Fö2019/01330). De fyra myndigheterna gavs i uppdrag att, inom ramen för NCSC, koordinera arbetet med att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter, förmedla råd och stöd när det gäller hot, sårbarheter och risker samt utgöra en nationell plattform för samverkan och informationsutbyte med privata och offentliga aktörer inom cybersäkerhetsområdet. Av uppdraget framgick att samverkan skulle utvecklas stegvis under perioden 2021–2023 och att de fyra uppdragsmyndigheterna skulle ha en nära samverkan med Försvarets materielverk, Polismyndigheten och Post- och telestyrelsen, vilka skulle ges möjlighet att medverka i NCSC:s verksamhet. Av uppdraget framgick också att regeringen avsåg att under 2023 ta ställning till hur NCSC:s verksamhet bör inriktas och bedrivas efter 2023. Regeringen konstaterar att det jämnt fördelade ansvaret för NCSC mellan flera olika myndigheter har bidragit till svårigheter med såväl styrning som uppföljning och ansvarsutkrävande. Regeringen delar därmed Riksrevisionens bedömning att det har varit svårt att nå en effektiv samverkan mellan myndigheterna under uppbyggnaden av NCSC. Regeringen vidtar därför flera åtgärder för att på sikt nå en effektiv samverkan inom NCSC.

Den 27 april 2023 gav regeringen FRA, MSB, Försvarsmakten och Säkerhetspolisen i uppdrag att inom ramen för NCSC stärka samverkan med näringslivet. I uppdraget ingår att genomföra en bred informationskampanj riktad till näringslivet samt etablera en särskild samverkan med vissa sektorer. Uppdraget syftar till att myndigheter och näringsliv ska arbeta aktivt och systematiskt med att utveckla sin informations- och cybersäkerhet för att uppnå ett fullgott skydd på området.

För att företag ska ges bättre förutsättningar att bedriva ett effektivt arbete inom området informations- och cybersäkerhet krävs det därutöver en utvecklad samverkan och ett stöd från de myndigheter som har ansvar inom området. En viktig del i detta är tillgången till lägesbilder. Regeringen gav därför den 27 april 2023 även de fyra ovannämnda myndigheterna i uppdrag att regelbundet utarbeta lägesbilder riktade till aktörer inom näringslivet, likaväl som till statliga myndigheter samt kommuner och regioner.

Försvarsdepartementet har utsett en utredare som kommer att biträda departementet och denne har fått i uppdrag att lämna förslag på hur en ändamålsenlig, effektiv organisering och styrning av cybersäkerhetscentret

ska utformas. Utredningen avser bl.a. att syfta till att ge NCSC bättre förutsättningar att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra större it-incidenter genom samverkan med såväl privata som offentliga aktörer. En del av utredarens uppdrag är att utreda hur FRA ska tilldelas ett huvudansvar för att leda samordningen, utvecklingen och genomförandet av centrets verksamhet. En utmaning för NCSC:s verksamhet har varit att de olika myndigheterna sinsemellan inte kan dela alla uppgifter som bedöms nödvändiga på grund av sekretess, vilket även Riksrevisionen påpekar i sin granskning. Utredaren ska därför analysera och föreslå hur ett nödvändigt utbyte av information med sekretesskyddade uppgifter bör hanteras inom centret och lämna förslag på eventuella författningsändringar. Utredaren ska också analysera hur informationsutbytet med både privata och offentliga aktörer inom cybersäkerhetsområdet bör hanteras.

Uppdraget ska redovisas till regeringen senast första halvåret 2024. Sammanfattningsvis konstaterar regeringen att Riksrevisionens iakttagelser och rekommendationer är ett välkommet bidrag för att uppnå en förstärkt informations- och cybersäkerhet. Som framgår ovan vidtar regeringen flera åtgärder i syfte att utveckla NCSC och stärka arbetet med informations- och cybersäkerhet i stort. Genom denna skrivelse anser regeringen att Riksrevisionens rapport är slutbehandlad.

Motionerna

Stärkt förmåga

Peter Hultqvist m.fl. (S) föreslår i kommittémotion 2023/24:2564 yrkande 60 att en övergripande nationell strategi för global cyberpolitik ska utarbetas för att ge en grund för ett samordnat beslutsfattande i staten.

I kommittémotion 2023/24:415 yrkande 7 föreslår Jimmy Ståhl m.fl. (SD) att säkerhetsrutinerna för viss it-infrastruktur ska ses över.

Emma Berginger m.fl. (MP) föreslår i kommittémotion 2023/24:2450 yrkande 5 att cybersäkerheten i offentlig sektor och särskilt samhällsviktiga delar av den privata sektorn ska stärkas.

I motion 2023/24:1903 av Peter Hedberg och Malin Larsson (båda S) föreslås att möjligheterna att stärka Sveriges förmåga att hantera tele- och cyberkrig, förbättra landets kapacitet att lagra nödvändiga resurser samt stärka våra centrala infrastruktursystem ska ses över.

Det nationella cybersäkerhetscentret

I kommittémotion 2023/24:422 yrkande 3 föreslår Tobias Andersson m.fl. (SD) att Nationellt cybersäkerhetscenters och andra myndigheters arbete för att förebygga, upptäcka och hantera cyberangrepp och it-incidenter ska utvärderas och eventuellt stärkas.

Mikael Larsson och Niels Paarup-Petersen (båda C) föreslår i följdmotion, tillika kommittémotion, 2023/24:2765 att samverkan mellan cybersäkerhetscentret och näringslivet ska stärkas (yrkande 1), och de anför att det för Sveriges medborgare och företag är It-brottscentrum, och inte cybersäkerhetscentret, som är den viktigaste aktören för att få hjälp mot cyberkriminalitet och cyberbrottslighet. Mer måste enligt motionärerna göras för att stärka förutsättningarna också för It-brottscentrum (yrkande 2).

It-haverikommission

Hanna Gunnarsson m.fl. (V) föreslår i kommittémotion 2023/24:461 yrkande 4 att en it-haverikommission bör tas fram i samarbete mellan berörda myndigheter.

Kunskapsuppbyggnad

Peter Hultqvist m.fl. (S) föreslår i kommittémotion 2023/24:2564 yrkande 59 att regeringen ska ta initiativ till kunskapsuppbyggnad inom cybersäkerhetsområdet i offentlig sektor.

I kommittémotion 2023/24:422 av Tobias Andersson m.fl. (SD) föreslås att ett effektivt informationsarbete ska bedrivas för att höja medvetenheten om hot, sårbarheter och risker (yrkande 4) och att antalet personer med informationssäkerhetskompetens ska öka för att stödja företag, den offentliga sektorn och andra organisationer (yrkande 7).

Rashid Farivar m.fl. (SD) föreslår i kommittémotion 2023/24:497 yrkande 12 att allmänhetens medvetande om AI och cyberresiliens ska stärkas.

I kommittémotion 2023/24:2450 av Emma Berginger m.fl. (MP) yrkande 7 föreslås att en eller flera myndigheter ska ges i uppdrag att ta fram en nationell strategi för stärkt motståndskraft mot desinformation och propaganda så att medie- och informationskunnigheten kan stärkas.

Markus Wiechel och Björn Söder (båda SD) föreslår i motion 2023/24:880 att det ska göras en bredare granskning av svenskarnas användning av teknik från länder som kan anses utgöra säkerhetshot.

Samverkan

Tobias Andersson m.fl. (SD) föreslår i kommittémotion 2023/24:422 att nätinfrastrukturens resiliens ska stärkas genom samarbete i kris mellan olika företag (yrkande 5) och att former för samverkan och informationsdelning mellan myndigheter och privata företag och organisationer ska utvecklas för att öka säkerheten (yrkande 6).

Outsourcing och upphandling

Jimmy Ståhl m.fl. (SD) förslår i kommittémotion 2023/24:415 yrkande 6 att upphandlingsförfaranden ska ses över för att säkerställa att informationsflöden och funktioner inte faller i orätta händer vid utbyggnad av viss it-infrastruktur.

I kommittémotion 2023/24:461 föreslår Hanna Gunnarsson m.fl. (V) att regeringen ska ta fram riktlinjer för hur outsourcing av it-verksamhet ska kunna undvikas i den statliga förvaltningen (yrkande 2). Motionärerna föreslår även att regeringen ska uppdra åt relevanta myndigheter att ta fram tydligare säkerhetskrav och villkor för upphandlingar på it-området (yrkande 3).

Molntjänster

Peter Hultqvist m.fl. (S) föreslår i kommittémotion 2023/24:2564 yrkande 17 att regeringen ska ta initiativ till att säkra statens insyn och kontroll över den säkerhetskänsliga information som förvaras i eller kan förvaras i molntjänster och servrar.

I kommittémotion 2023/24:461 av Hanna Gunnarsson m.fl. (V) yrkande 6 föreslås att regeringen snarast ska utreda och återkomma med ett förslag till statliga molntjänster där data och program ska kunna lagras på ett säkert sätt.

Internationellt regelverk

Hanna Gunnarsson m.fl. (V) föreslår i kommittémotion 2023/24:461 yrkande 1 att Sverige ska verka för ett internationellt regelverk kring cybersäkerhet.

Utskottets ställningstagande

Utskottet anser att flera åtgärder vidtagits de senaste åren för en förbättrad informations- och cybersäkerhet i samhället, i Sverige och inom EU, men att uppdraget långt ifrån är slutfört. Utskottet välkomnar därför Riksrevisionens senaste granskning i fråga om samhällets informations- och cybersäkerhet och instämmer i slutsatsen att det bör skapas en strategisk, holistisk och långsiktig inriktning för det fortsatta arbetet.

Utskottet ser därför positivt på det åtgärder som regeringen aviserar i skrivelsen, t.ex. arbetet med att ta fram en ny informations- och cybersäkerhetsstrategi som ligger i linje med Europaparlamentets och rådets olika initiativ. Att denna nationella strategi harmonierar med andra eventuellt angränsande strategier är mycket viktigt, vilket också regeringen anför. Av vikt är även stödet till och samverkan med statliga myndigheter och näringsliv.

En annan viktig komponent i ett framgångsrikt informations- och cybersäkerhetsarbete är kompetensutvecklingen på området. Regeringen konstaterar att det tyvärr råder brist på just sådan kompetens i samhället i stort. Regeringen förutser breda och långsiktiga insatser för att komma till rätta med dessa utmaningar, också genom EU:s försorg, vilket utskottet välkomnar.

MSB:s arbete i sammanhanget bör också nämnas eftersom myndigheten bl.a. regelbundet genomför kunskapshöjande aktiviteter, t.ex. utbildningar riktade mot chefer och informationssäkerhetsansvariga inom kommuner, regioner, kommun- och regionägda bolag samt myndigheter.

Utskottet ser även positivt på den resurstillförsel och omorganisation som regeringen tillför bl.a. Regeringskansliet för att stärka arbetet med

informations- och cybersäkerhet. Utskottet vill här särskilt lyfta fram inrättandet av ett nationellt säkerhetsråd för informationsutbyte och strategisk samordning i frågor som rör nationell säkerhet, vilket bedöms bl.a. kunna ge goda förutsättningar att uppnå en samlad styrning och effektiva former för samordning av informations- och cybersäkerhetsfrågorna.

Sist men inte minst – mot bakgrund av Riksrevisionens iakttagelser – välkomnar utskottet de åtgärder som syftar till att ytterligare förstärka det nationella cybersäkerhetscentrets verksamhet när det gäller organisering och styrning, bl.a. till förmån för samverkan med näringslivet och utvecklade lägesbilder. Det nya nationella cybersäkerhetscentret får redan i dag ändå ses som ett mycket viktigt steg framåt, och utskottet ser fram emot att ta del av centrets fortsatta utveckling, t.ex. i fråga om att utreda och dra lärdom av större it-relaterade incidenter, förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter, främja it-incidentrapportering m.m.

Utskottet vill i sammanhanget passa på att framhålla att det är viktigt att det vid upphandling av elektronisk kommunikation och andra it-relaterade tjänster – liksom på många andra områden – ställs krav på att inköp görs på ett systematiskt och strategiskt sätt som säkerställer leveranssäkerhet och krisberedskap. Utskottet välkomnar Upphandlingsmyndighetens arbete med att ge förstärkt stöd vid upphandlingar av samhällsviktig verksamhet samt MSB:s arbete med att stödja aktörer inom den offentliga sektorn i informationssäker upphandling.

Avslutningsvis önskar utskottet återigen framhålla att ett stärkt psykologiskt försvar skapar förutsättningar för att värna det öppna och demokratiska samhället och för att säkerställa försvarsviljan. I dagsläget ser man mycket ofta exempel på hur påverkanskampanjer används för att undergräva ett land och olika organisationer men även enskilda människor. Utskottet anser därför att Myndigheten för psykologiskt försvar är av stor vikt för den fortsatta utvecklingen av samhällets krisberedskap och det civila försvaret. I sammanhanget bör också vikten av samhällets informations- och cybersäkerhet fortsätta att beaktas.

Därmed ser utskottet sammantaget inte skäl till att vidta några ytterligare åtgärder för tillfället i fråga om informations- och cybersäkerhet. De aktuella motionsyrkandena avstyrks därför. Utskottet föreslår att riksdagen lägger regeringens skrivelse till handlingarna.

Reservationer

1. Stärkt förmåga, punkt 1 (S)

av Peter Hultqvist (S), Johan Andersson (S), Erik Ezelius (S), Markus Selin (S) och Lena Johansson (S).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 1 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2023/24:2564 av Peter Hultqvist m.fl. (S) yrkande 60 och
avslår motionerna
2023/24:415 av Jimmy Ståhl m.fl. (SD) yrkande 7,
2023/24:1903 av Peter Hedberg och Malin Larsson (båda S) och
2023/24:2450 av Emma Berginger m.fl. (MP) yrkande 5.

Ställningstagande

Det svenska cyberförsvaret och beredskapen för cyberangrepp måste stärkas. Det är i dag viktigare än någonsin tidigare att både myndigheter, kommuner och företag bedriver ett systematiskt informationssäkerhetsarbete. Det är av särskild vikt att stärka samhällets förmåga att möta asymmetriska cyberhot. Den nationella cyberkompetensen bl.a. inom offentlig sektor behöver stärkas för att kunna bemöta cyberangrepp och antagonistiska cyberhot. Angreppen från cyberkriminella blir allt vanligare samtidigt som vi ser att angreppen även ökar från främmande stater. Främmande stater har resurser att skada samhällsviktiga funktioner, såsom livsmedelsförsörjning, elförsörjning och sjukvård, med långvariga samhällsstörningar som följd. Vi föreslår sålunda att en övergripande nationell strategi för global cyberpolitik ska utarbetas för att ge en grund för ett samordnat beslutsfattande i staten. I arbetet med strategin bör en haverikommission för cyberincidenter övervägas. Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

2. Stärkt förmåga, punkt 1 (MP)

av Emma Berginger (MP).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 1 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2023/24:2450 av Emma Berginger m.fl. (MP) yrkande 5 och
avslår motionerna
2023/24:415 av Jimmy Ståhl m.fl. (SD) yrkande 7,
2023/24:1903 av Peter Hedberg och Malin Larsson (båda S) och
2023/24:2564 av Peter Hultqvist m.fl. (S) yrkande 60.

Ställningstagande

Det sätt på vad modern krigföring utnyttjar svagheter i samhället bidrar aktivt till polarisering och oro som kan användas för att kontrollera att samhället styrs på ett sätt som passar olika aktörers egna syften. Påverkan på opinionen i Sverige och i andra länder i syfte att destabilisera samhället sker fortlöpande. Det sker genom att öka motsättningarna mellan grupper. Många aktörer är intresserade av detta. Ryssland och Kina är exempel på stormakter som bedriver sådan verksamhet mot hela EU, och extremistiska rörelser ideologiskt baserade på religion eller annan övertygelse har splittring som mål och medel i sin verksamhet. Påverkan består bl.a. av att ifrågasätta demokratisk legitimitet och rättsstatens principer, att sprida extrema åsikter och rena lögner samt att polarisera den offentliga debatten. Desinformation sprids på olika internetplattformar av både stater, privatpersoner och organisationer för att tjäna pengar. Särskilt i krissituationer utnyttjas människors rädsla och oro. Cyberangrepp pågår från flera olika aktörer. Kina är ett exempel på en stormakt som bedriver avancerat cyberspionage för att främja sin egen ekonomiska utveckling och utveckla sin militära förmåga. Det sker genom omfattande underrättelseinhämtning och stöld av teknologi, forskning och utveckling. De flesta angrepp mot digitala system sker av ekonomiska skäl och en mindre andel sker av militära eller politiska skäl. Även om syftet med de flesta angrepp är brottslighet i ekonomiskt syfte kan resultatet ändå bli allvarliga störningar av stora och viktiga verksamheter i samhället, och svagheterna i infrastrukturen kan utnyttjas för angrepp på en stat. Cybersäkerheten behöver därför höjas i alla verksamheter i samhället i både offentlig och privat sektor, och Sverige behöver stärka sin förmåga att förebygga och bemöta cyberattacker. Att den digitala infrastrukturen är global och tillgänglig är avgörande för att företag och organisationer ska kunna bedriva sin verksamhet och dela kunskap mellan människor i olika länder. En

öppen värld gynnar Sverige på många sätt och är en förutsättning för att miljöhot och säkerhetshot ska kunna hanteras. Mot bakgrund av det anförda föreslår jag att cybersäkerheten i offentlig sektor och i särskilt samhällsviktiga delar av den privata sektorn ska stärkas. Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

3. Det nationella cybersäkerhetscentret, punkt 2 (C)

av Mikael Larsson (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 2 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2023/24:2765 av Mikael Larsson och Niels Paarup-Petersen (båda C) yrkandena 1 och 2 samt
avslår motion
2023/24:422 av Tobias Andersson m.fl. (SD) yrkande 3.

Ställningstagande

Riksrevisionen har dragit allvarliga slutsatser om regeringens styrning av samhällets informations- och cybersäkerhet. Regeringens och Regeringskansliets arbetsmetoder har inte varit effektivt utformade och det saknas strategiska avvägningar och prioriteringar som inriktar verksamheten. Allvarligt är att regeringen inte har vidtagit åtgärder när myndigheterna inte nått samsyn i arbetet med att ta fram en gemensam nationell modell för informations- och cybersäkerhet inom ramen för samverkansgruppen och informationssäkerhet och det nationella cybersäkerhetscentret (NCSC). Riksrevisionen bedömer bl.a. att det saknas tillräcklig operativ och taktisk kunskap om hur cybersäkerhetsarbetet bedrivs på myndigheter och inom den privata sektorn samt att mycket av resurserna inom Regeringskansliet gått åt till att hantera olika EU-initiativ, utan att Sverige för den sakens skull driver någon sammanhållen linje på EU-nivå. Vidare visar Riksrevisionens granskning på att vissa aktörer inte upplever sig inkluderade i arbetet, exempelvis näringslivet, samt att det finns problem med att utreda it-relaterade brott, att ge stöd till olika aktörer vid incidenter och att bristen på kompetens i samhället kopplat till informations- och cybersäkerhet även fortsättningsvis är kritisk.

När det gäller it-relaterad brottslighet konstaterar Riksrevisionens rapport att det finns problem med att utreda sådan brottslighet. Polisen har i uppdrag att höja förmågan att hantera cyberbrottslighet. Det finns mycket att göra och en åtgärd kan vara att förenkla anmälningar av cyberbrottslighet till e-

anmälningar, något som skulle möjliggöra en nationell lägesbild och hantering. För Sveriges medborgare och företag är det It-brottscentrum, och inte cybersäkerhetscentret, som är den viktigaste aktören för att få hjälp mot cyberkriminalitet och cyberbrottslighet. Därför kan cybersäkerhetscentret inte ses som den enda spjutspetsen i kampen mot cyberhot. Mer måste göras för att stärka förutsättningarna också inom It-brottscentrum.

Jag föreslår sammanfattningsvis att samverkan mellan cybersäkerhetscentret och näringslivet ska stärkas och att regeringen ska verka för att It-brottscentrum, inte cybersäkerhetscentret, ska vara den viktigaste aktören för att få hjälp mot cyberkriminalitet och cyberbrottslighet. Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

4. It-haverikommission, punkt 3 (V)

av Hanna Gunnarsson (V).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 3 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2023/24:461 av Hanna Gunnarsson m.fl. (V) yrkande 4.

Ställningstagande

Alla statliga myndigheter ska i dag rapportera allvarliga it-incidenter till MSB. Syftet är bl.a. att skapa förutsättningar för att vidta rätt skyddsåtgärder och utveckla förmågan att förebygga och hantera framtida incidenter. Det är bra och viktigt. Jag menar att omfattande it-incidenter i högre grad behöver rapporteras, följas upp och granskas i en sammanhållen process. Det gäller alla större incidenter med en samhällelig påverkan, även lokalt. Obligatoriet omfattar myndigheter, men även andra organisationer kan välja att rapportera frivilligt. Här finns utrymme för att öka privata aktörers vilja att delta i rapporteringen. Jag föreslår utifrån det anförda att en it-haverikommission ska bildas i samarbete mellan berörda myndigheter. Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

5. Kunskapsuppbyggnad, punkt 4 (S)

av Peter Hultqvist (S), Johan Andersson (S), Erik Ezelius (S), Markus Selin (S) och Lena Johansson (S).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 4 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2023/24:2564 av Peter Hultqvist m.fl. (S) yrkande 59 och
avslår motionerna
2023/24:422 av Tobias Andersson m.fl. (SD) yrkandena 4 och 7,
2023/24:497 av Rashid Farivar m.fl. (SD) yrkande 12,
2023/24:880 av Markus Wiechel och Björn Söder (båda SD) och
2023/24:2450 av Emma Berginger m.fl. (MP) yrkande 7.

Ställningstagande

Det svenska cyberförsvaret och beredskapen för cyberangrepp måste stärkas. Det är i dag viktigare än någonsin tidigare att både myndigheter, kommuner, och företag bedriver ett systematiskt informationssäkerhetsarbete. Det är av särskild vikt att stärka it- och cybersäkerheten samt samhällets förmåga att möta asymmetriska cyberhot. Den nationella cyberkompetensen behöver stärkas för att kunna bemöta dessa cyberangrepp och antagonistiska cyberhot. Vi föreslår därför att regeringen ska ta initiativ till kunskapsuppbyggnad inom cybersäkerhetsområdet inom offentlig sektor. Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

6. Kunskapsuppbyggnad, punkt 4 (MP)

av Emma Berginger (MP).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 4 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2023/24:2450 av Emma Berginger m.fl. (MP) yrkande 7 och
avslår motionerna
2023/24:422 av Tobias Andersson m.fl. (SD) yrkandena 4 och 7,
2023/24:497 av Rashid Farivar m.fl. (SD) yrkande 12,
2023/24:880 av Markus Wiechel och Björn Söder (båda SD) och

2023/24:2564 av Peter Hultqvist m.fl. (S) yrkande 59.

Ställningstagande

Desinformation innebär avsiktligt spridande av falsk eller vilseledande information för att åstadkomma skada eller påverka människors attityder, ställningstaganden och handlande i en viss riktning. Desinformation sprids med syftet att exempelvis skada förtroendet för Sverige och det öppna demokratiska samhället. För att möta hotet från desinformation krävs insatser från många myndigheter och aktörer. Det krävs dock en samordning. I betänkandet Det demokratiska samtalet i en digital tid – Så stärker vi motståndskraften mot desinformation, propaganda och näthat (SOU 2020:56) förordas att en nationell strategi för stärkt motståndskraft mot desinformation, propaganda och näthat tas fram. Stora sociala medier har tagit fram och börjat använda policyer för att markera när yttranden från ledare strider mot etablerade fakta. Arbetet med detta behöver intensifieras och gemensamma principer som utgår från Europakonventionen behöver fastställas av EU. Med anledning av det anförda föreslår jag att en eller flera myndigheter ska ges i uppdrag att ta fram en nationell strategi för stärkt motståndskraft mot desinformation och propaganda så att medie- och informationskunnigheten kan stärkas. Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

7. Outsourcing och upphandling, punkt 6 (V)

av Hanna Gunnarsson (V).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 6 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2023/24:461 av Hanna Gunnarsson m.fl. (V) yrkandena 2 och 3 samt
avslår motion
2023/24:415 av Jimmy Ståhl m.fl. (SD) yrkande 6.

Ställningstagande

Det dominerande påbudet är att allt fler it-områden ska läggas ut på entreprenad. En politisk vilja till ökad outsourcing av it-tjänster måste sättas i relation till vilka säkerhetsrisker det kan medföra. 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. Om upphandlingar på it-området ändå sker måste tydliga säkerhetskrav finnas med redan i inledningsskedet. Det är centralt att

både beställare och köpare har nödvändig kompetens för att avgöra vilka säkerhetslösningar som krävs. Krav såväl som genomförande bör också så långt det är möjligt granskas av en oberoende aktör. Jag föreslår därför att regeringen ska ta fram riktlinjer för hur outsourcing av it-verksamhet ska kunna undvikas i den statliga förvaltningen, så långt det är möjligt och att regeringen ska ge relevanta myndigheter i uppdrag att ta fram tydligare säkerhetskrav och villkor för upphandlingar på it-området. Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

8. Molntjänster, punkt 7 (S)

av Peter Hultqvist (S), Johan Andersson (S), Erik Ezelius (S), Markus Selin (S) och Lena Johansson (S).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 7 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2023/24:2564 av Peter Hultqvist m.fl. (S) yrkande 17 och
avslår motion
2023/24:461 av Hanna Gunnarsson m.fl. (V) yrkande 6.

Ställningstagande

Digitala infrastrukturer är av yttersta vikt på många sätt både i normalläge och vid kris eller krig. Digitaliseringen av ledning och verkan är av central betydelse i dagens krigföring. Att kunna använda s.k. molntjänster är en förutsättning för den krigförande förmågan. Exempelvis använder såväl den ukrainska staten som Försvarsmakten molntjänster för att göra informationen oåtkomlig för fienden. Information och data har flyttats utanför landets gränser. Från ett svenskt perspektiv är detta ett område där lösningar måste sökas. Det är i sammanhanget oerhört angeläget att den svenska statens insyn och kontroll säkras. Vi föreslår därför att regeringen ska ta initiativ till att säkra statens insyn och kontroll över den säkerhetskänsliga information som förvaras i eller kan förvaras i molntjänster och servrar. Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

9. Molntjänster, punkt 7 (V)

av Hanna Gunnarsson (V).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 7 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2023/24:461 av Hanna Gunnarsson m.fl. (V) yrkande 6 och
avslår motion
2023/24:2564 av Peter Hultqvist m.fl. (S) yrkande 17.

Ställningstagande

Att lagra data digitalt över internet via ett s.k. moln blir allt vanligare och tillämpas i stor utsträckning i offentlig sektor. Men det finns stora säkerhetsutmaningar med detta. Statens servicecenter har redan 2017, i rapporten En gemensam statlig molntjänst för myndigheternas it-drift, föreslagit en säker hantering av data genom en statlig molntjänst i form av statligt ägda serverhallar för lagring åt offentlig sektor. Statens servicecenter konstaterar också att en molntjänst bör ha sitt säte utanför storstadsområdena för att stärka säkerheten och öka effektiviseringen för att sänka kostnaderna. Vänsterpartiet anser vidare att ett statligt moln också skulle kunna hantera lagringen åt privata företag, och verksamheten skulle på sikt kunna bli lönsam för staten. Det gäller i synnerhet samhällsviktiga företag vars verksamhet är av särskild vikt att skydda. Dessvärre har regeringen agerat saktfärdigt och inkonsekvent, och någon statlig molnlösning har ännu inte sett dagens ljus. Jag föreslår därför att regeringen snarast ska återkomma med ett förslag till en eller flera statliga molntjänster där data och program ska kunna lagras på ett säkert sätt. Molntjänsterna ska också, mot en rimlig avgift, kunna hantera lagring åt andra aktörer än staten, om så önskas. Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

10. Internationellt regelverk, punkt 8 (V)

av Hanna Gunnarsson (V).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 8 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion

2023/24:461 av Hanna Gunnarsson m.fl. (V) yrkande 1.

Ställningstagande

Internationellt samarbete är helt nödvändigt för en fungerande cybersäkerhet. Oavsett hur stark den nationella säkerheten på cyberområdet är, måste frågan om cybersäkerhet oundvikligen betraktas som en internationell sådan. Det handlar både om hur stater själva agerar mot varandra och hur stater agerar gentemot andra aktörer. Inom EU finns direktiv om nät- och informationssäkerhet (NIS och NIS2) som omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster. Men det saknas fortfarande ett gemensamt internationellt regelverk kring cybersäkerhet. Jag föreslår därför att regeringen ska verka för att ett internationellt regelverk kring cybersäkerhet tas fram. Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

BILAGA

Förteckning över behandlade förslag

Skrivelsen

Regeringens skrivelse 2023/24:26 Riksrevisionens rapport om regeringens styrning av samhällets informations- och cybersäkerhet.

Följdmotionen

2023/24:2765 av Mikael Larsson och Niels Paarup-Petersen (båda C):

1. Riksdagen ställer sig bakom det som anförs i motionen om samverkan mellan cybersäkerhetscentret och näringslivet och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om it-brottscentrum och tillkännager detta för regeringen.

Motioner från allmänna motionstiden 2023/24

2023/24:415 av Jimmy Ståhl m.fl. (SD):

6. Riksdagen ställer sig bakom det som anförs i motionen om säker upphandling och utbyggnad av viss it-infrastruktur och tillkännager detta för regeringen.
7. Riksdagen ställer sig bakom det som anförs i motionen om säkerhetsrutiner för viss it-infrastruktur och tillkännager detta för regeringen.

2023/24:422 av Tobias Andersson m.fl. (SD):

3. Riksdagen ställer sig bakom det som anförs i motionen om att utvärdera och eventuellt stärka arbetet genom Nationellt cybersäkerhetscenter och andra myndigheter för att förebygga, upptäcka och hantera cyberangrepp och it-incidenter och tillkännager detta för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om att bedriva ett effektivt informationsarbete för att höja medvetenheten om hot, sårbarheter och risker och tillkännager detta för regeringen.
5. Riksdagen ställer sig bakom det som anförs i motionen om att nätinfrastrukturens resiliens ska stärkas genom samarbete i kris mellan olika företag och tillkännager detta för regeringen.

6. Riksdagen ställer sig bakom det som anförs i motionen om att utveckla former för samverkan och informationsdelning mellan myndigheter och privata företag och organisationer för att öka säkerheten och tillkännager detta för regeringen.
7. Riksdagen ställer sig bakom det som anförs i motionen om att öka antalet personer med informationssäkerhetskompetens för att stödja företag, den offentliga sektorn och andra organisationer och tillkännager detta för regeringen.

2023/24:461 av Hanna Gunnarsson m.fl. (V):

1. Riksdagen ställer sig bakom det som anförs i motionen om att Sverige ska verka för ett internationellt regelverk kring cybersäkerhet och tillkännager detta för regeringen.
2. 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.
3. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör uppdra åt relevanta myndigheter att ta fram tydligare säkerhetskrav och villkor för upphandlingar på it-området samt på oberoende granskning och tillkännager detta för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om att en it-haverikommission bör tas fram i samarbete mellan berörda myndigheter och tillkännager detta för regeringen.
6. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen snarast bör utreda och återkomma med ett förslag till statliga molntjänster där data och program ska kunna lagras på ett säkert sätt och tillkännager detta för regeringen.

2023/24:497 av Rashid Farivar m.fl. (SD):

12. Riksdagen ställer sig bakom det som anförs i motionen om att stärka allmänhetens medvetande om AI och cyberresiliens och tillkännager detta för regeringen.

2023/24:880 av Markus Wiechel och Björn Söder (båda SD):

Riksdagen ställer sig bakom det som anförs i motionen om en bredare granskning av svenskarnas användning av teknik från länder som kan anses utgöra säkerhetshot, och detta tillkännager riksdagen för regeringen.

2023/24:1903 av Peter Hedberg och Malin Larsson (båda S):

Riksdagen ställer sig bakom det som anförs i motionen om att se över möjligheterna att stärka Sveriges förmåga att hantera tele- och cyberkrig,

förbättra landets kapacitet att lagra nödvändiga resurser samt stärka våra centrala infrastruktursystem och tillkännager detta för regeringen.

2023/24:2450 av Emma Berginger m.fl. (MP):

5. Riksdagen ställer sig bakom det som anförs i motionen om att stärka cybersäkerheten i offentlig sektor och särskilt samhällsviktiga delar av den privata sektorn och tillkännager detta för regeringen.
7. Riksdagen ställer sig bakom det som anförs i motionen om att en eller flera myndigheter bör ges i uppdrag att ta fram en nationell strategi för stärkt motståndskraft mot desinformation och propaganda så att medie- och informationskunnigheten kan stärkas och tillkännager detta för regeringen.

2023/24:2564 av Peter Hultqvist m.fl. (S):

17. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör ta initiativ till att säkra statens insyn och kontroll över den säkerhetskänsliga information som förvaras i eller kan förvaras i molntjänster och servrar och tillkännager detta för regeringen.
59. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör ta initiativ till kunskapsuppbyggnad inom cybersäkerhetsområdet i offentlig sektor och tillkännager detta för regeringen.
60. Riksdagen ställer sig bakom det som anförs i motionen om att en övergripande nationell strategi för global cyberpolitik som ger grund för ett samordnat beslutsfattande i staten bör utarbetas och tillkännager detta för regeringen.

Tryck: Elanders Sverige AB, Vällingby 2023