Kommittémotion

Motion till riksdagen 2017/18:4139

av Andreas Carlson m.fl. (KD)

med anledning av prop. 2017/18:205 Informationssäkerhet för samhällsviktiga och digitala tjänster

Förslag till riksdagsbeslut

1. Riksdagen ställer sig bakom det som anförs i motionen om att inrätta en svensk cybersäkerhetsmyndighet och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om att ge denna myndighet tillsynsansvar i frågor som gäller cyber- och informationssäkerhet och tillkännager detta för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om att ge denna myndighet ett ansvar att ta fram de föreskrifter som ska styra svenskt cyber- och informationssäkerhetsarbete och tillkännager detta för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om att ge denna myndighet ett operativt ansvar för att implementera dessa föreskrifter och tillkännager detta för regeringen.

Motivering

Regeringen har lagt fram en proposition för att genomföra NIS-direktivet i svensk lagstiftning. Detta har sin bakgrund i att Europaparlamentet och rådet 2016 antagit ett direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverk och informationssystem inom hela EU, det s.k. NIS-direktivet. I syfte att genomföra NIS-direktivet i svensk rätt föreslår regeringen en ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster.

Den nya lagen innebär bl.a. att vissa leverantörer av samhällsviktiga och digitala tjänster ska vidta säkerhetsåtgärder till skydd för säkerheten i nätverk och informationssystem: att leverantörerna ska rapportera incidenter som påverkar kontinuiteten i tjänsterna, att den myndighet som regeringen bestämmer ska utöva tillsyn över att lagen och föreskrifter som har meddelats i anslutning till den följs och

ska kunna besluta om vitesföreläggande och sanktionsavgift mot den som inte följer lagens bestämmelser.

Hoten mot den svenska cybersäkerheten torde vid det här laget vara välbekanta. Skandalen på Transportstyrelsen, Polismyndighetens beslut att frångå säkerhetsskyddsförordningen, Uppdrag granskning avslöjande att cancerbehandlingen på Akademiska sjukhuset i Uppsala stängts av med en cyberattack och det faktum att Myndigheten för press, radio och tv betalat lösensummor till it-utpressare är alla exempel på hur utsatta vi är. Lägg där till att Sverige enligt FRA varje dag drabbas av attacker från främmande makt, att MSB rapporterat in 260 it-incidenter och att upp till 10 000 attacker bedöms begås mot svenska intressen varje månad.

Attackerna kan begås av kriminella, terrorister eller stater med en fientlig inställning mot Sverige. I Försvarsberedningens rapport står att ”ett systematiskt informations- och cybersäkerhetsarbete är nödvändigt för att samhällets aktörer ska kunna upprätthålla en väl avvägd cyberförmåga i totalförsvaret”. I dag är det systematiska arbetet uppdelat bland en mängd olika myndigheter, vilket också beredningen konstaterar: ”Det ställs krav på aktörernas informations- och cybersäkerhet från t.ex. MSB, Säpo, Datainspektionen, Post- och telestyrelsen. Med NIS-direktivets införande kommer även sektorsansvariga myndigheter att utöva tillsyn och då ökar risken ytterligare för ineffektiv verksamhet och otydlighet i roller och ansvar. Sammanlagt innebär detta att vi kommer ha sex stycken olika tillsynsmyndigheter för informations- och cybersäkerhet. Försvarsberedningen anser att regeringen bör se över hur tillsyn och övervakning gällande informations- och cybersäkerhet i samtliga civila sektorer ska samordnas.”

Kristdemokraterna delar insikten att den svenska cyber- och informationssäkerheten är i stort behov av förbättring. NIS-direktivet innebär att sådana steg har tagits på EU-nivå och vi är positiva till detta. Vi delar regeringens uppfattning att en ny lag krävs för att adekvata säkerhetsåtgärder ska vidtas för att skydda säkerhet i nätverk och informationssystem, att incidentrapportering ska ske samt behovet av goda föreskrifter, en bra uppföljning och tillsyn och behovet av viten och sanktioner mot den som bryter mot detta. Det vore också väl värt att beakta det arbete Sverige gör inom Iso-standardiseringen, där vi varit med och tagit fram ledande standarder för styrning av cybersäkerhet, som Iso/IEC 27001. När krav ställs på privata aktörer gällande cyber- och informationssäkerhet kan dessa standarder innebära ett effektivare och enklare sätt att ställa krav än ny lagstiftning eftersom de är antagna europeiska standarder som utgör norm på området. Vi delar däremot inte regeringens hållning att det är lämpligt att dela upp detta ansvar på flera olika myndigheter.

Regeringens förslag innebär en fragmentering av det svenska arbetet med cybersäkerhet och saknar dessutom en modell för operativt stöd. Fragmenteringen består i att sex olika myndigheter, Statens energimyndighet, Transportstyrelsen, Finansinspektionen, Inspektionen för vård och omsorg, Livsmedelsverket och Post- och telestyrelsen alla föreslås bli tillsynsmyndigheter. Det innebär att samma kompetens och parallella arbetsmetoder för att åstadkomma samma sak ska upprättas på sex olika myndigheter, i stället för att koncentreras till en egen myndighet. Att utöva tillsyn kring cyber- och informationssäkerhet kräver expertkunskap, och sådan kunskap är både hett eftertraktad och relativt sällsynt. En tillsynsmyndighet behöver vara en attraktiv arbetsplats som erbjuder spetskompetens. Vi ser en betydande risk att detta inte uppnås om arbetet inte samlas under samma tak.

Bristen på operativt stöd är ett annat problem. En del i NIS-direktivet innebär att alla länder ska inrätta ett organ för incidenthantering, ett Computer Security Incident Response Team, i propositionen kallad CSIRT-enhet, dit incidenter kan rapporteras. Det är av yttersta vikt att påpeka att denna enhet inte kommer att bidra med ett operativt stöd för att hantera de incidenter som samhällsviktiga aktörer rapporterar in. Vi menar att detta är en stor brist i regeringens förslag och att en cybersäkerhetsmyndighet också bör agera som ett operativt stöd. Det är ett annat skäl till att inte fragmentisera tillsynsarbetet. Vi anser att en svensk cybersäkerhet bör ha ett stort mandat att agera, och därmed krävs också en stor samlad kompetens.

Vår syn, baserad på forskning och utbyte med näringsliv och myndigheter, är att det inte är ändamålsenligt eller kostnadseffektivt att låta de många olika sektorsmyndigheterna ha tillsynsansvaret för nätverks- och informationssäkerhet inom respektive sektor. Det finns flera problem med den föreslagna ordningen. För det första finns det en överhängande risk att sektorsmyndigheterna inte kommer att kunna säkra den kompetens som krävs för en god tillsyn eftersom omfattande kompetensbrist råder på marknaden. För det andra kommer tillsynsorganisationer och revisionsmetodik i onödan att utvecklas på olika håll, vilket driver kostnader. För det tredje går de stordriftsfördelar som kan uppnås genom att en och samma tillsynsmyndighet handhar all tillsyn förlorade. Slutligen blir det stor gränsdragningsproblematik mellan myndigheter som exempelvis MSB, Säkerhetspolisen, Datainspektionen, PTS och sektorsmyndigheterna – där ett och samma it-system och verksamhetsdel kan täckas in av flera olika krav kring säkerhetsåtgärder, incidentrapportering och tillsyn. Man kan förvänta sig överlappningar samt att delar faller mellan olika ansvarsområden.

I stället bör all tillsyn gällande informationssäkerhet och dataskydd – för samtliga civila sektorer och gentemot samtliga författningar – koncentreras till en cybersäkerhetsmyndighet. Tillsynen skulle riktas enligt sektorsmyndigheternas behov och resultatet av tillsynen och incidentrapporter skulle delas med dem.

Kristdemokraterna anser att den fragmentariska organiseringen av cybersäkerheten minskar vår förmåga att skydda oss mot hot mot vår cyber- och informationssäkerhet. Varje enskild myndighet med tillsynsansvar är i sig för liten och arbetar mot en för avgränsad sektor för att kunna upprätthålla den samlade kompetens och förmåga som krävs för att skydda hela samhället. Cybersäkerhet är en expertkunskap och den behöver samlas på en plats, en egen cybersäkerhetsmyndighet.

Vi föreslår att en sådan myndighet ska ha ett mycket brett uppdrag. Cybersäkerhet är inte enbart en militär fråga, utan den är också i allra högsta grad aktuell för försörjning av el och vatten, banksystem m.m. Vi föreslår därför en stegvis uppbyggnad av myndigheten.

- Samla ansvaret för tillsyn i cybersäkerhetsfrågor. I dag delas ansvaret mellan flera olika myndigheter och ännu fler föreskrifter från dessa myndigheter. En enskild myndighet med samlad kompetens löser uppgiften bättre än ett lapptäcke av tillsynsmyndigheter med helt andra huvuduppdrag.
- Samla och renodla de föreskrifter som finns. Dagens myndigheter ger ut en mängd olika föreskrifter. Samma företag eller myndighet kan få delar av sin cybersäkerhet granskad av flera olika aktörer mot flera olika föreskrifter. Det är inte ändamålsenlig styrning. Föreskrifterna bör i ett senare skede ersättas med cybersäkerhetsmyndighetens egna, mer ändamålsenliga föreskrifter. Dessa bör i sin tur vara målstyrande och beskriva vad som ska uppnås, inte hur detta ska uppnås.

- Ett operativt metodstöd. När cybersäkerhetsmyndigheten utövar tillsyn för en myndighet eller ett företag och kommer med en åtgärdslista, bör den också ha ett uppdrag att bidra med metodstöd kring hur myndigheter eller företag ska uppnå målen. Eftersom cybersäkerhetsmyndigheten kommer att ha en stor del av den samlade kompetensen på området bör de också ha ett ansvar för och ett uppdrag att se till att andra klarar av målen.

I försvarsbeslutet från 2015 står att den samlade svenska förmågan att förbygga, motverka och aktivt hantera konsekvenser av civila och militära hot, händelser, attacker och angrepp i cybermiljön måste utvecklas och förstärkas. Regeringen anför vidare att ett svenskt cyberförsvar kräver samordning och koordinering av kompetenser, samt utpekade och inövade beslutsvägar, mellan olika myndigheter och samhällsfunktioner.

Kristdemokraterna menar att svaret på den frågan stavas en ny cybersäkerhetsmyndighet.

Andreas Carlson (KD)

Sofia Damm (KD)

Mikael Oscarsson (KD)

Tuve Skånberg (KD)