Kommittémotion

Motion till riksdagen 2017/18:306

av Mikael Oscarsson m.fl. (KD)

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

Förslag till riksdagsbeslut

Riksdagen ställer sig bakom det som anförs i motionen om att införa en myndighet för cybersäkerhet och tillkännager detta för regeringen.

Motivering

Regeringen skriver att det finns ett stort behov av att utveckla samhällets informations- och cybersäkerhet. För detta tar man fram en nationell strategi för samhällets informations- och cybersäkerhet. Regeringen beskriver att huvudsyftena med strategin är att bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet samt att höja medvetenheten och kunskapen i hela samhället och stödja de insatser och det engagemang som redan finns i samhället för att stärka informations- och cybersäkerheten.
Vårt samhälle, liksom de flesta samhällen i världen, är och blir alltmer beroende av informationsteknik. Det kan gälla datorbaserad styrning och övervakning av viktiga samhällsfunktioner som t.ex. elförsörjning, vattendistribution, trafikreglering på vägar, järnvägar och i luften eller hantering av andra funktioner som betalningar, handel och information.

Cyberangrepp kan leda till mycket omfattande följder för samhället, i vissa avseenden lika förödande som ett angrepp med konventionella vapen. Till skillnad från konventionella angrepp kan det vara utomordentligt svårt att identifiera vem som står bakom ett cyberangrepp. Frågan uppstår också, om man kan se cyberangrepp som en krigshandling, som kan besvaras med konventionell vapenmakt. Sannolikt inte, då cyberattacker har en inbyggd osäkerhet som bl.a. gör att man aldrig med säkerhet kan veta vem som ytterst initierat angreppet. Hot om cyberangrepp kan dessutom utnyttjas i utpressningssyfte – inte bara mot företag och organisationer utan även mot regeringar. Samhället måste därför ha en god förmåga såväl att möta direkta angrepp som att

avskräcka en eventuell angripare. Det kan bara ske på samma arena som hotet uppträder – cyberarenan.

Systemet för informationssäkerhet, precis som det svenska krissystemet i övrigt, bygger på två grundprinciper: ansvars- och närhetsprincipen. Närhetsprincipen betyder att en kris först och främst ska hanteras där den inträffar av de närmast berörda och ansvariga. Ansvarsprincipen innebär att den som bedriver verksamheten i vanliga fall även är ansvarig i en krissituation. Om de lokala resurserna inte räcker till och om hanteringen av incidenten blir för omfattande kan statliga insatser bli aktuella. Att cyberhotet sällan kan avgränsas geografiskt eller till en enskild verksamhet innebär att staten ofta kommer att spela en viktig, ibland avgörande, roll.

Det finns sex myndigheter i Sverige som har ett av regeringen utsett ansvar för informationssäkerheten i samhället. Dessa myndigheter ingår i Samverkansgruppen för informationssäkerhet (Samfi). Att benämna Samfi som Sveriges cyberförsvar vore inte korrekt. Den är först och främst inriktad mot Sveriges informationssäkerhet och hantering av it-incidenter. De myndigheter som ingår i Samfi är: Myndigheten för samhällsskydd och beredskap (MSB), Försvarsmakten (FM), Försvarets materielverk (FMV), Försvarets radioanstalt (FRA), Rikspolisstyrelsen (RPS) (som representeras genom Rikskriminalpolisen och Säkerhetspolisen) samt Post- och telestyrelsen (PTS). MSB har främsta ansvaret för informationssäkerheten i Sverige. De övriga myndigheternas aktivitetsområden är främst av stödjande och förebyggande karaktär.

Ett problem med skyddet mot cyberhot är att mycket av infrastrukturen och handeln och andra funktioner är beroende av företag eller ägs av företag. Dessa är vinstdrivande och i vissa fall obenägna att satsa stora medel i förebyggande syfte då det är svårt att värdera nyttan i förväg. Detta kan jämföras med kostnader för försäkringar eller för våra gemensamma samhällsfunktioner som brandkåren eller Försvarsmakten. Samhället måste därför införa regler och även vidta andra åtgärder för att underlätta för företag som är beroende av datorbaserad systemstyrning och övervakning samt tvinga dem att vidta förebyggande åtgärder som minskar samhällets sårbarhet mot hot och angrepp inom cyberdomänen.

Det ligger i sakens natur att det inte är möjligt att förutse hur eventuella cyberattacker kan se ut om man själv inte bedriver forskning och försök när det gäller hur cyberattacker kan genomföras. Kan man inte agera aktivt mot en angripare kan redan organisationer eller stater med tämligen små resurser överbelasta våra system eller ostört söka svagheter i vårt skydd mot cyberattacker. Det är därför angeläget att vi utvecklar en egen förmåga att aktivt motverka cyberattacker. Därför ser Kristdemokraterna positivt på att regeringen nu gett Försvarsmakten i uppdrag att arbeta fram ett förslag till cyberförsvar.

En förutsättning för att vidta såväl passiva som aktiva motåtgärder är att det finns en organisation med bred kompetens. Det innebär bl.a. att alla myndigheter, företag och organisationer måste ha en skyldighet att rapportera alla former av cyberangrepp som riktas mot dem till en central myndighet. Detta är ett nödvändigt led för att skapa den kunskapsbredd som krävs för att möta olika typer av cyberangrepp. Det är dock omöjligt att skapa ett rimligt skydd mot cyberangrepp utan omfattande internationell samverkan rörande olika aspekter av cyberhotet. Även denna samverkan skulle underlättas om den hanterades av en för ändamålet utpekad organisation.

En sådan organisation skulle också ha en viktig roll genom att ge råd om hur man skyddar sig mot cyberangrepp till de företag, myndigheter och organisationer vars verksamhet är starkt beroende av fungerande it-system. En speciell aspekt på

cyberkrigföring är den roll som den spelar i militära sammanhang. De flesta moderna vapensystem är i dag beroende av avancerad informationsteknologi, t.ex. satellitnavigering, radarsystem och informationsöverföring. Det innebär att det mesta av militär verksamhet kräver såväl kvalificerat skydd mot cyberangrepp som att angrepp mot en motståndares informationssystem kan ge mycket stora fördelar.

Cybersäkerhet är dock så mycket mer än ett aktivt skydd mot antagonister som har för avsikt att förstöra ett annat lands it-infrastruktur. Cybersäkerhet handlar också om att värja sig mot fel och brister i system som gör att system oplanerat stängs av eller slutar att producera på grund av okända fel och brister. Detta har vi t.ex. sett vid tillfällen då flygplatsradar och kommunikationer slagits ut och flygplan fått dirigeras om eller inte haft möjlighet att lyfta/landa. Detta är ytterst problematiskt och påvisar både en brist på systemresiliens och en uppenbar brist på redundans.

Med dagens system är det möjligt att bygga in både resiliens och redundans utan att man nödvändigtvis behöver ha flera olika kompletta system för samma uppgift. Detta är ett arbete regeringen borde se över för samhällskritiska system såsom flygplatsers kritiska system, betalningskritiska system, ledningssystem för blåljusmyndigheter samt andra system som kan klassas som kritiska för samhällets grundfunktionalitet.

För att möta dessa problem och de problem som tas upp i propositionen räcker regeringens förslag på åtgärder inte särskilt långt. Kristdemokraterna vill se att en särskild myndighet med ansvar för Sveriges cybersäkerhet inrättas. Detta bör ges regeringen till känna.

Mikael Oscarsson (KD)

Andreas Carlson (KD)

Sofia Damm (KD)

Tuve Skånberg (KD)