SOFF
Säkerhets- och försvarsföretagen

Ju2015/2650/SSK

Remiss på betänkandet SOU 2015:23 ”Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten”

Allmänt om utredningen
Säkerhets- och försvarsföretagen har inbjudits att lämna synpunkter på betänkandet ”Informations- och cybersäkerhet i Sverige - Strategi och åtgärder för säker information i staten” (SOU 2015:23). SOFF välkomnar i allt väsentligt utredningens förslag och stöder den övergripande slutsatsen att det behövs en strategi för statens informations- och cybersäkerhet nedbrutna på de sex angivna delmålen. Det finns stora behov att koordinera, stärka och vitalisera metoder och arbetssätt för att möta de hot och risker som samhället står inför på informationssäkerhetsområdet.

SOFF vill framhålla betydelsen av att tydliga ansvarsförhållanden mellan berörda parter och myndigheter upprättas såväl horisontellt som vertikalt i syfte att uppnå en god funktionalitet. De oklara ansvarsförhållandena har även haft en hämmande effekt för utvecklandet av en effektiv marknad. Företagen har i flera fall erfarit att det saknats statliga interlokutör för att behandla långsiktiga och strategiska frågeställningar på informationssäkerhetsområdet samt att upphandlingsprocesserna på detta område är mycket fragmenterade.

I detta sammanhang är det också viktigt att påpeka att ökade pålagor på företagen genom höjda certifieringskostnader skulle försvåra marknadsinträdet framförallt för små och mellanstora företag. Vidare är det från SOFF:s perspektiv angeläget att lagverken är tydligt utformat för att undvika divergerande tolkningar mellan skilda aktörer syfte att förenkla och ensa upphandlingsprocesser.

Styrning, organisation och inriktning
SOFF är positivt till stärkt styrning och tillsyn av informationssäkerheten inom ramen för statens verksamhet samt att statliga aktörer blir tydligare kravställare vid upphandlingar. Vidare är det utmärkt att utredningen tydligt uttalar att Sverige ska vara en stark internationell partner på cyber- och informationssäkerhetsområdet. Sverige har en, i internationell jämförelse, mycket kompetent och konkurrenskraftig IT-sektor. Vidare är behovet av internationell samverkan växande inte minst med USA som till stora delar leder den snabba teknikutvecklingen på detta område.

Betänkandet innehåller även bra förslag om utökad dialog kring kompetensförsörjningen med näringslivet vilket SOFF välkomnar. En mycket viktig detalj är att utredningen föreslår att det är regeringen som bör leda IT-säkerhetsarbetet. Det är även bra att utredningen tittar på hur kryptoförmågan ska säkras och samhällsviktig verksamhet skyddas. SOFF ställer sig positivt till utredningens förslag att MSB, FRA, FMV och Försvarsmakten ges i uppdrag att utveckla processen för säkra kryptografiska funktioner i enlighet med det gemensamma dokument som myndigheterna presenterat.

Dessvärre belyser inte utredningen tillräckligt utförligt näringslivets och framförallt forskning- och teknikutvecklingens roll i dessa sammanhang. Som utredningen framhåller har Sverige en världsledande kryptoindustri. Det skapar ett betydande säkerhetspolitiskt mervärde för Sverige och

tillgodoser att landet inte behöver utveckla osunda beroendeförhållanden till utländska aktörer. Vårdandet av den internationella konkurrenskraften och tillväxtfrämjande åtgärder för denna industri bör därför särskilt beaktas från statliga aktörer. Exempel på sådana åtgärder kan handla om utformandet av exportfrämjande åtgärder, riktade satsningar på forskning och teknikutveckling samt utvecklade dialogformer mellan företag och myndigheter i tidiga faser av nya utvecklingsprojekt. Just utvecklandet av tidiga dialoger mellan användare och leverantör skapar förutsättningar för leverantören att bidra med insikt och kunskap men även möjlighet att ställa frågor för att bättre förstå nuläget och framtida behov hos kunden.

SOFF välkomnar också utredningens förslag om en obligatorisk IT-incidentrapportering för samtliga statliga myndigheter. Det skulle stärka förmågan att förebygga och hantera IT-incidenter samt ge en bättre strategisk överblick om de problem och utmaningar som föreligger på detta område. En sådan överblick skapar även bättre förutsättningar för marknaden att identifiera nya tekniska och kostnadseffektiva lösningarna som behovsägaren kan disponera. Men det bör även övervägas införa samma krav på rapportering från kommuner och landsting i syfte att ytterligare stärka denna förmåga.

SOFF är samtidigt oroat över att utredningen inte närmare föreslår åtgärder för de bristande resurser och förmåga samhället har att hantera de säkerhetspolitiska dimensionerna av området. Trots vissa klargörande är det även för olika områden oklara roller mellan myndigheterna. Det gap som finns med samverkan med näringslivet mellan offentligt/privat, utförare/tjänster adresseras utan konkreta åtgärder och nödvändiga satsningar. En strategisk dialog mellan dessa aktörer är av stort värde. Men det krävs också utökad kunskap, forskning och övning samt resursallokering i detta syfte.

Bristande resurser och förmåga

SOFF noterar en ökad medvetenhet om att företag och övriga delar av samhället är starkt beroende av cyber- och informationssäkerhet, samhällsviktig verksamhet och grundläggande infrastruktur på området. Betänkandet konstaterar att staten för närvarande har brister i förutsättningarna för att förebygga och hantera hot och risker inom detta område. SOFF delar den uppfattningen.

För att arbetet med informationssäkerhet ska vara effektivt krävs det kunskap, forskning och analysverksamhet om olika former av hot och risker samt vilka skyddsåtgärder som myndigheterna bör vidta mot detta. Det finns därför ett antal företeelser vilket SOFF gärna sett att betänkandet mer utförligt belyst så som bl.a. att sociala medier används för att störa yttrandefriheten och skapa desinformation; att sofistikerade och till del statsstödda intrång och genomförs mot cybernätverk Sverige i första hand för att skaffa ekonomisk fördel samt för stöld av immateriella rättigheter och känslig marknadsinformation samt den ökade politiserade "hacktivism verksamhet” som syftar till att exponera känslig information. För dessa hot med säkerhetspolitisk betydelse krävs verktyg och förmåga. Det är något som SOFF anser till del saknas idag. Det saknas dock inte bara kunskap om hoten, utan även om vilka åtgärder som behöver vidtas. Vi upplever här att myndigheterna har betydande utmaningar i att värdera hoten, väga säkerhetsbehoven och följaktligen då även vida de åtgärder som är nödvändiga.

Det föreslås också att MSB ska få en utökad roll i på informationssäkerhetsområdet vilket kräver en anslagshöjning som enligt utredningen eventuellt kan finansieras genom en omfördelning inom utgiftsområde 06. SOFF har inga invändningar mot en utökad roll för MSB i detta sammanhang. Men i ljuset av de neddragningar som redan gjorts på myndigheten samt det stora tryck som finns på

utgiftsområde 06 (Försvar och samhällets krisberedskap) som en konsekvens av det nya försvarsbeslutet och den försämrade säkerhetspolitiska utvecklingen krävs det att externa medel tillförs till MSB utanför ramanslaget till utgiftsområde 06.

Samverkan med näringslivet
Samhällets säkerhet har stor funktionell och ekonomisk betydelse för företagen. Till exempel är tillgången till en robust infrastruktur en internationell konkurrensfördel för företag som är verksamma i Sverige. Företag kan antas ha ett intresse av att ta del av de offentliga aktörernas kunskaper om olika hot och risker, varför offentliga aktörer med ansvar för IT-säkerhet bör även överväga vilket behov företagen har av utbildningar, kunskap, övning och vägledningar som det offentliga kan erbjuda, för att nå ett säkrare, mer robust samhälle. SOFF föreslår att staten bjuder in företag och branschorganisationer för att gemensamt identifiera mål och åtgärder för arbetet med informationssäkerhet, inte minst gemensamma övningar och utbildningar.

Vidare skulle en utökad samverkan med näringslivet kunna uppnås genom att myndigheterna och näringslivet gemensamt, men med respekt för de skilda rollerna mellan kund och leverantör, sjösätter ett antal mindre pilotprojekt på cyber- och informationssäkerhetsområdet som utmanar traditionella upphandlingsmodeller. Dessa pilotprojekt skulle bygga på att företagen kommer in på ett tidigt stadium i utvecklingsfaser samt ett intensivt informations- och erfarenhetsutbyte inför och under projektens genomförande. Syftet med dessa pilotprojekt skulle vara att utveckla effektivare upphandlingsmodeller med målsättningen att uppnå större kundnöjdhet hos slutanvändaren och effektivare resursanvändning från företagens sida.

För Säkerhets- och försvarsföretagen

Robert Limmergård
Generalsekreterare