Stockholms universitet

2022-01-05 Dnr SU-FV-21-3413-21

Juridiska fakultetskansliet Försvarsdepartementet

Remiss: Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)

Juridiska fakultetsnämnden välkomnar de synpunkter och förslag som lämnas i betänkandet av Cybersäkerhetsutredningen (*Sveriges säkerhet - behov av starkare skydd för nätverks- och informationssystem*, SOU 2021:63). Juridiska fakultetsnämnden instämmer i den slutsats som Cybersäkerhetsutredningen presenterar, att det finns allvarliga brister i informations- och cybersäkerheten och att det finns behov av national styrning och samordning vid framtagande av en gemensam hot-, sårbarhets- och riskbedömning till stöd i arbetet med informations- och cybersäkerhet. Betänkandet skisserar en detaljerad och komplicerad verklighetsbild beträffande såväl den pågående digitalisering av samhällsviktiga funktioner och det haltande arbetet med att stärka informations- och cybersäkerheten i förhållande till samhällets ökade sårbarhet. Betänkandet belyser teknikens och digitaliseringens dubbla karaktär, d.v.s. ju mer datoriserat samhället blir desto mer sårbart blir det för olika antagonistiska hot. Förhållandet kompliceras av att många samhällsviktiga system är uppkopplade till samt styrs via internet.

I tillägg till detta vill fakultetsnämnden framhålla några frågor som bör analyseras framgent.

1. Det kan inte nog betonas hur viktig utbildningen av människor är i förhållande till skapandet av ett bra skydd mot cyberangrepp. Betänkandet tar ett systemperspektiv och fokus ligger på rutiner kring och samordning av de system som i många verksamheter är att betrakta som säkerhetskänsliga. I detta sammanhang nämns nätverks- och informationssystem. Det kan argumenteras att den beskrivningen förbiser människors betydelse, dels i bemötandet av olika hot och cyberangrepp, dels som en potentiell svaghet i en totalförsvarspolicy. Beträffande människor som riskfaktor kan nämnas ”social manipulation”. En skyddskedja är bara så stark som den svagaste länken och i många fall är det människor som är den svagaste länken. Inte alla avstår från att klicka på okända länkar eller stoppa in upphittade USB-minnen i en arbetsdator, bara för att nämna några exempel. Vikten av rollen som utbildning spelar i sammanhanget får således inte glömmas bort, även om det kan vara naturligt att fokusera samordningen kring tekniska lösningar i första hand. Beträffande människor som en del i bemötandet

Juridiska fakultetsnämnden

Stockholms universitet
106 91 Stockholm

Besöksadress:
Universitetsvägen 10 A

Telefon: 08 16 24 68
E-post: karolina.alveryd@juridicum.su.se

av ett cyberangrepp kan nämnas att vilka hot och cyberangrepp som kan aktualiseras i framtiden inte är möjligt att förutse. Oklart är också vilka tekniska åtgärder som kommer att finnas tillgängliga för att bemöta cyberangrepp. En viktig samordningsfunktion för myndigheterna blir därför att agera som brygga mellan statliga och privata aktörer så att de tekniska lösningar som finns vid den tidpunkten, särskilt i den privata sektorn, på kort varsel kan anpassas för att bemöta framtida hot och cyberangrepp.

2. Betänkandet betonar vikten av att säkerhetskänsliga verksamheter uppfyller särskilda krav för att upprätthålla skyddet av sådana verksamheter. Tanken är att detta ska ske genom uppfyllandet av särskilda krav i förhållande till IKT-produkter, -tjänster och -processer. Fakultetsnämnden vill dock understryka att ett bra försvar mot cyberangrepp inte bara kan fokusera på verksamhetsrelaterade, egna system. Att en verksamhets nätverks- och informationssystem lever upp till vissa systemkrav ska egentligen vara den sista försvarslinjen mot olika angrepp. Här kan lyftas fram vikten av att tidigt kunna upptäcka cyberhot och cyberangrepp, exempelvis ute på internet, eller fall där liknande verksamheter attackeras.

3. Ett centralt begrepp i förhållande till skyddet av nätverks- och informationssystem är tillit. Utan tillit till de myndigheter som är ansvariga för tillsyn av de krav som ställs för att uppnå ett gott försvar finns en risk att satsningen inte når sina mål. Enligt betänkandet är Säkerhetspolisen och Försvarsmakten samrådsmyndigheter som ska ha vissa befogenheter i förhållande till en verksamhetsutövare av säkerhetskänslig verksamhet enligt säkerhetsskyddslagen. Detta innebär en möjlighet för dessa samrådsmyndigheter att få tillgång till verksamhetsutövarnas nätverks- och informationssystem. Som framgår av betänkandet finns ingen etablerad legaldefinition av vad som avses med verksamhet som är känslig för Sveriges säkerhet och vad som ryms inom begreppet ”säkerhetskänslig verksamhet” (s. 61). Även civil samhällsverksamhet är enligt betänkandet av betydelse för Sveriges säkerhet. Detta kan till exempel avse verksamheter i näringslivet. Med barkund av detta måste hänsyn tas till att olika verksamheter inom näringslivet kan ha olika inställning till vilka samrådsmyndigheter som bör ha tillgång till deras nätverks- och informationssystem. Exempelvis bör en lokal verksamhet som försörjer Sverige med el acceptera att samrådsmyndigheter med kopplingar både till säkerhetstjänsten och till försvarsmakten har insyn i deras system. En bank som har internationella kunder och där bankens renommé beträffande integritet och sekretess är viktigt, kan ha svårare att acceptera sådan insyn. I avsnitt 5.3 av betänkandet nämns banker som måltavla av vissa cyberangrepp som har ett ekonomiskt syfte (s. 118). Med den osäkerheten som råder kring vad en säkerhetskänslig verksamhet är, måste det ifrågasättas i vilken utsträckning vissa privata aktörer inom näringslivet kommer att välkomna att samrådsmyndigheterna i form av Säkerhetspolisen och Försvarsmakten eventuellt får tillgång till deras nätverks- och informationssystem. Internationell erfarenhet har visat att vissa verksamheter, till exempel banker, kan vara känsliga för att samrådsmyndigheter med starka band till säkerhetstjänsten har tillgång till deras informationssystem. Om det offentliggörs att en bank ger en myndighet inom

säkerhetstjänsten tillgång till sina informationssystem, kan det skapa negativ publicitet som kan vara mer förödande för bankens verksamhet än ett cyberangrepp.

4. En med tillitsfrågan sammanhängande fråga är den om Säkerhetspolisen och Försvarsmakten är de mest lämpliga samrådsmyndigheterna ur ett tillitsperspektiv. Det kan argumenteras för att ”civila” myndigheter, d.v.s. myndigheter med svagare band till säkerhetstjänsten skulle kunna öka tilliten till samrådsförfarandet i förhållandet till verksamheter inom näringslivet som har ett stort behov av att utåt signalera att de tar kundsekretess och kundernas integritet på allvar. Här handlar det om att myndigheter förknippade med säkerhetstjänsten kan anses vara mindre transparenta jämförd med andra myndigheter. En åtgärd för att skapa ökad tillit skulle kunna vara att en ”civil” samrådsmyndighet utses, som vid behov kan vidarebefordra särskilda problem eller utmaningar till den myndighet som har kunskapen att ta hand om problemet, till exempel Säkerhetspolisen om det handlar om ett hot mot Sveriges säkerhet.

5. Enligt ändringsförslaget till säkerhetsskyddslagen (2018:585) är det verksamhetsutövaren som ska göra en säkerhetsbedömning om en driftsättning eller en förändring i ett informationssystem är lämpligt utifrån en säkerhetsskyddssynpunkt. Detta kräver i sin tur att det är tydligt om en viss verksamhet ryms inom begreppet ”säkerhetskänslig verksamhet”. Som förslaget är utformat är begreppet ”säkerhetskänslig verksamhet” förenligt med tolkningssvårigheter. Man kan tänka sig att bedömningen kan vara subjektiv och att en bedömning av huruvida en verksamhet som säkerhetskänslig kan varierar från en person till en annan. Därför bör de personer som hos en verksamhetsutövare ska ansvara för bedömningen för om verksamheten ryms inom begreppet säkerhetskänslig verksamhet identifieras. Vidare kan tolkningssvårigheter uppstå gällande tillämplig lag. I betänkandet hänvisas till NIS-direktivet som använder begreppet ”samhällsviktiga tjänster” och Säkerhetsskyddslagen som använder begreppet ”samhällsviktig verksamhet”. Frågan är i vilket utsträckning en ”samhällsviktig tjänst” enlig NIS-direktivet också kan betraktas som en ”samhällsviktig verksamhet”.

Sammanfattningsvis är Juridiska fakultetsnämndens av uppfattningen att betänkandet ger en övertygande bild om läget kring informations- och cybersäkerhet i förhållande till de hot om cyberangrepp som finns. Fakultetsnämnden är också överlag positivt inställd till de åtgärder som Cybersäkerhetsutredningen föreslår för att öka informations- och cybersäkerheten i förhållande till säkerhetskänsliga verksamheter. De synpunkter som har tillagts här ska tolkas som förslag att komplettera de åtgärder som har föreslagits samt att belysa gränsdragningsproblem som kan uppstå.

Remissvaret har på fakultetsnämndens uppdrag beslutats av dekanus, professor Jessika van der Sluijs. Yttrandet har beretts av universitetslektor Stanley Greenstein. Föredragande har varit Karolina Alveryd. Yttrandet har expedierats av Juridiska fakultetskansliet.

Jessika van der Sluijs

Karolina Alveryd