Till Statsrådsberedningen, Försvarsdepartementet, Justitiedepartementet och Näringsdepartementet

2020-04-23

Näringslivets syn på Sveriges kommande nationella cybersäkerhetscenter

Säkerhets- och försvarsföretagen (SOFF) och Teknikföretagen stödjer initiativet att inrätta ett svenskt nationellt cybersäkerhetscenter. Organisationerna välkomnar det förslag som de fyra utpekade myndigheterna presenterade i den rapport som överlämnades till regeringen i december 2019. Vi vill understryka vår förståelse för att såväl rapporten som de inkluderade förslagen återspeglar de givna förutsättningar som kringgärdar bildandet av centret.

Ambitionen med denna skrivelse är att bistå i centrets arbete.

Den målbild vi ser för Sveriges nationella cybersäkerhetscenter är att centret på ett trovärdigt sätt ska bidra till att stärka Sveriges samlade cybersäkerhet och cyberförsvar. Detta uppnås genom tillräcklig resurstilldelning, tydlig ansvarsfördelning och mandat för centret som den primära och samlande nationella aktören i dessa frågor. För att detta ska kunna realiseras behöver följande aspekter beaktas:

- Cybersäkerhetscentret – den primära och samlande nationella aktören
- Trovärdighet byggs genom ömsesidig dialog
- Handlingsutrymme kan uppnås genom substantiell finansiering
- Näringslivets konkurrenskraft måste ses som skyddsvärd
- Operativ verksamhet är prioriterad
- Fullgod kapacitet kräver bemanning dygnet runt

Cybersäkerhetscentret – den primära och samlande nationella aktören

I det förslag som i december 2019 presenterades uttrycks ”*…cybersäkerhetscentret ska höja den nationella förmågan genom samordnat agerande, informationsdelning och kunskapsöverföring…*”, detta ger utrymme för tolkning kring ansvarsfördelning mellan de olika involverade myndigheterna och hur strukturen för ledning kommer att fungera. Den enskilt viktigaste frågan i skapandet av det nationella cybersäkerhetscentret är att centret har ett eget tydligt mandat samt en instruktion som centret kan agera utifrån.

Vid en allvarlig IT-incident med ett snabbt händelseförlopp behöver *en* aktör kunna träda fram som har det övergripande beslutsmandatet. I det presenterade underlaget är det något oklart hur de olika styrgrupperna kommer att förhålla sig till varandra, deras beslutsmandat och deras relation till ledningen för centret. Det uttrycks att: ”*Centrets produkter fastställs i konsensus…*” samt att ”*chefen för centret ska också rådgöra med den operativa styrgruppen…*”. Formuleringar likt dessa pekar på att flera aktörer behöver vara inblandade för att beslut ska fattas.

Teknikföretagen
Box 5510, 114 85 Stockholm
Storgatan 5, Stockholm
Telefon 08-782 08 00
www.teknikforetagen.se

Centret bör ha en chef satt att leda centret som vet att hen direkt kan agera med full kraft för att hantera nationella cybersäkerhetsrelaterade allvarliga händelser. Den person som utses till chef ska kunna agera med centrets alla resurser och vid behov få stöd från ingående organisationer med extra tillförda resurser om så krävs. Det får inte uppstå en situation där en allvarlig cyberincident behöver beredas med respektive deltagande organisation innan centret kan agera. Det är önskvärt att det finns tydliga uppgifter och processer för arbetet i centret och att den person som utses till chef för centret har erfarenhet från såväl de myndigheter som ingår i centret som Regeringskansliet och gärna från näringslivet.

Vi vill understryka betydelsen av att de rådgivande grupper som - enligt förslaget ska knytas till centret och bestå av externa intressenter - tillmäts värde och ses som partners. Detta kommer att kräva en kontinuitet, en löpande involvering i arbetet, ett förtroende mellan involverade aktörer och att de råd som ges respekteras och omhändertas.

Centrala uppgifter för cybercentret som vi önskar lyfta

Nedanstående är ett antal centrala uppgifter för cybercentret som vi önskar lyfta. Om uppgifterna nedan leds av centret kommer det att vara tydligt för alla berörda aktörer att det är cybercentret som har att hantera Sveriges samlade cyberinsatser.

1. Säkerställa tidskritisk och relevant informationsdelning mellan deltagande parter,
2. Operativ koordinering och händelsehantering,
3. Samarbete om analyser och framtagandet av för landet gemensam lägesbild,
4. Utarbetandet och samanställningen av strategiska analyser och att ta fram en för landet samlad hot- och riskbild,
5. Utarbetandet av en nationell hanterings- och beredskapsplan för att tydliggöra olika aktörers ansvar och var man ska vända sig vid en allvarlig cyberincident,
6. Koordinera samverkan med nationella och internationella partner.

Trovärdighet byggs genom ömsesidig dialog

De resultat som önskas uppnås genom centrets arbete kan inte en aktör lösa på egen hand utan det bygger på ett långsiktigt arbete, under förtroendefulla förhållanden med både offentliga och privata aktörer involverade. Vi önskar en ömsesidig dialog och en gemensam arbetsprocess som tar Sverige framåt i arbetet kring stärkt cybersäkerhet.

Svenska företag och branscher har alla olika behov och vi är fullt medvetna om att inte alla dessa kan tillgodoses direkt; det är varken möjligt ekonomiskt eller tidsmässigt. Likväl ser vi det som prioriterat att de som har ansvar för centret är tydligare i sin avgränsning och explicit anger hur de ser att näringslivet ska involveras i det löpande arbetet – operativt och strategiskt. Som alla nya organisationer behöver centret ett visst mått av arbetsro för att kunna bygga upp gemensamma processer och därigenom hitta sin roll och sitt arbetssätt. Detta har vi full förståelse för. Vad vi dock vill poängtera är vikten av att centret *redan initialt* inkluderar näringslivet i sitt arbete. Om ambitionen är att centret *vid full utbyggnad* ska kunna stödja näringslivet så måste näringslivet involveras från början för att delge sina behov samt tydliggöra hur de kan bistå. En struktur skapar en kultur och om vissa relevanta aktörer utelämnas redan från början

kommer denna kultur att institutionaliseras. Det är särskilt viktigt att uppmärksamma de teknikintensiva företagen som, i hög utsträckning, är föremål för främmande makters intresse men som i traditionell mening inte betraktats som skyddsvärda.

Vidare behövs det mekanismer för att kunna hantera det faktum att det finns företag som har strategisk betydelse i Sverige och har utländska ägare. Önskvärt vore en modell där relevanta branschorganisationer, tillsammans med ett urval av företag, ges plats direkt i centret, i linje med vad som sker i Norge.

Vi vill tydliggöra att det inte är färdiga produkter i form av exempelvis checklistor som är det mest prioriterade för näringslivet; det görs redan från exempelvis både MSB och Teknikföretagen. Vad som krävs och efterfrågas av centret är en kontinuerlig dialog som baseras på ett ömsesidigt informationsutbyte.

Handlingsutrymme kan uppnås genom substantiell finansiering
Finansieringen är inte allt, men krävs för att skapa handlingsutrymme. Om centret ska formeras på basis av befintliga medel kommer utrymmet för nya initiativ vara strikt begränsat. I praktiken kommer det innebära att varje myndighet bidrar till centrets verksamhet efter egen förmåga och budget, vilket inte ger en önskvärd långsiktighet utan skapar stor risk för osäkerhet i fråga om finansiering. Vi noterar också att ingående myndigheter, liksom övriga aktörer som associeras med centret, inte förefaller se någon radikal effekthöjning genom ett center, följaktligen är de i begränsad utsträckning intresserade av att allokera resurser för att verksamheten ska kunna expandera eller växa organiskt.

Ur vårt perspektiv har säkerhetsarbete i hela samhället varit underfinansierat under en period. En önskvärd och rimlig nivå i termer av finansiering är därför att centret skyndsamt tillförs de medel som myndigheterna beskriver i sin rapport till regeringen, och att dessa medel faktiskt tillförs, och inte tas från nuvarande verksamhet hos berörda myndigheter.

Vår bedömning är att med de medel som efterfrågas kan centret snabbt bli operativt och skala upp i enlighet med den plan som angivits i det myndighetsgemensamma förslaget. Substantiell finansiering krävs också för att näringslivet ska inkluderas i en rimlig utsträckning och ses som en prioriterad partner. Vår bestämda uppfattning är att den typ av samverkan som beskrivs och eftersträvas i slutrapporten inte går att göra utan tillskjutna medel.

Näringslivets konkurrenskraft är skyddsvärd
Arbetet i centret bör bygga på ett brett perspektiv av säkerhet. Utöver traditionell nationell säkerhet bör även ekonomisk säkerhet och konkurrenskraft bejakas. Om svenska företag inte inkluderas i centrets arbete i ett initialt skede riskerar centrala aspekter för den svenska konkurrenskraften, i realiteten, att vara exkluderade från centrets arbete. Detta riskerar att skada Sveriges teknologiska ledarskap. Svenska företag ligger idag i framkant i industriell teknik och innovation. Detta faktum önskar vi att myndigheter och departement bejakar genom att ge det stöd de kan när attackerna kommer från stater eller statsunderstödda aktörer. Många företag har sina servrar fulla med forskningsresultat, utvecklingsprojekt och patentansökningar. Dessa representerar enorma värden för den stat som vill ta genvägar i sin egen näringslivs- och teknikutveckling. I praktiken kan det innebära att de företag som utvecklat ny teknik konkurreras ut av sina egna lösningar, realiserade av företag i de länder som ägnar sig åt

cyberattacker. Vi vill också understryka att det rör sig om reella hot som redan skadar näringslivet avsevärt. Enligt svensk underrättelse- och säkerhetstjänst har antalet statsunderstödda cyberangrepp kontinuerligt ökat samtidigt som angriparnas metoder utvecklats och blivit allt mer sofistikerade. Nära hälften av Teknikföretagens medlemmar uppger exempelvis att de identifierat cyberattacker under de senaste två åren. Konsekvenserna av attackerna är också tydliga i form av driftsavbrott och att känslig information röjts eller förstörts. Uppskattningsvis kostar attackerna näringslivet ca 16 miljarder kr per år, och de teknikintensiva sektorerna av ekonomin är särskilt utsatta. [1] [2]

Operativ verksamhet är prioriterad

Som vi redogjort för ovan är det viktigt att centret får en tydlig målbild och en realistisk handlingsplan med fokus på det operativa arbetet. Detta kan bidra till fokus, stringens och transparens. Det behöver dock framhållas att cybervärlden med dess hot och antagonister är så pass föränderlig att en alltför detaljrik strategi väldigt snabbt kommer att bli förlegad. Medan det är enkelt att förutspå att antalet attacker kommer att öka är det svårare att projicera vilken typ av attacker, hot och sårbarheter som kommer att upptäckas. Det är inte heller självklart vilka aktörer under en given tid, statliga eller privata, som kommer att behöva stöd.

Med beaktande av ovanstående bör handlingsplanen som centret tar fram vara dynamisk och ta hänsyn till den föränderliga värld som den har att agera i. Med det sagt måste den operativa verksamheten påbörjas samtidigt som den strategiska. Vad som sker i det operativa formar det strategiska och vice versa. På så sätt definieras vad centret *är* genom vad det *gör*. Vi förordar därför att centret har en hög grad av pragmatism inledningsvis, vilket i sin tur kräver att det ges tillräckligt med mandat för att kunna agera självständigt och snabbt.

Fullgod kapacitet kräver bemanning dygnet runt

Cyberattacker tar inte långhelg och så borde inte det nationella cybersäkerhetscentret göra. Hotaktörerna slår till i rätt tidszon och ofta efter kontorstid, vilket ett center måste beakta och kunna bemöta. Vi ser även hur fler attacker styrs av AI-liknade funktionalitet som varken sover eller tar lunchrast utan är aktiva dygnet runt.

Vid en allvarlig cyberattack krävs snabbt agerande, både för att hantera och minimera skada samt för att krishantera och minimera oro och osäkerhet. Önskvärt är därför att det nationella cybersäkerhetscentret har en kapacitet och en bemanning att vara aktivt dygnet runt årets alla dagar. Samarbete bör också sökas med de etablerade säkerhetsföretag som bedriver s.k. MSS/SOC verksamhet, flera av dessa har också verksamhet dygnet runt, året runt.

---

[1] Estimerat baserat på uppgifter från Teknikföretagens medlemmar samt IBM, 2019 Cost of Databrech Report, 2019, FRA, ”Fakta om IT-angrepp”, 2018 samt McAffe, "Economic Impact of Cybercrime - No Slowing Down", 2017

[2] Se även Evertiq, “Så mycket kommer it-attacken mot Addtech att kosta”, https://evertiq.se/news/38250 samt Atea; ”Eftercyberangreppet mot norsk hydro”, https://www.atea.se/it-specialisten/sakerhet/efter-cyberangreppet-mot-norsk-hydro/

Vad gör vi inom ramen för Teknikföretagen och Säkerhets- och försvarsföretagen?

- Tagit fram en basguide om cybersäkerhet. (TF) https://www.teknikforetagen.se/globalassets/i-debatten/publikationer/cybersakerhet/skydda-din-it-miljo---en-guide-till-medvetet-sakerhetsarbete-i-mindre-teknikforetag.pdf

- Informationsmaterial om hotbilden. (TF) https://www.teknikforetagen.se/branschfragor/digitalisering/cybersakerhet/ samt (SOFF) https://soff.se/wp-content/uploads/2018/03/Cybersecurity_statsunderst%C3%B6dda-akt%C3%B6rer.pdf

- Ordnar regional turné tillsammans med Säpo för att öka den grundläggande kunskapen kring cyberattacker, cyberhotet och vad aktörer kan göra på egen hand. (SOFF+TF)

- Ordnar nationell konferens kring hur cybersäkerhet kan kopplas till värdekedjor, innovationsflöden och integration mellan förtagen. (SOFF+TF)

- Bedriver gemensamt arbete för ökad medvetenhet om cybersäkerhet på europeisk nivå genom samarbetsorganisationen Orgalim. (TF)

- Arrangerar årligen Cyberförsvarsdagen tillsammans med Försvarsmakten, FRA och MSB för att möjliggöra kontaktytor mellan näringsliv och myndigheter. Cyberförsvarsdagen samlar varje år ca 250 deltagare med en jämn representation från det privata och det offentliga. (SOFF)

- Driver ett forum för delning av hotinformation mellan företagen med syfte att etablera en förtroendefull miljö mellan olika aktörer. (SOFF) På sikt skulle detta kunna bli en samarbetspartner till centrets forum för delning av hotinformation.

- Arbetar löpande med ett 20-tal initiativ, bland annat med Teknikföretagen, för att stärka att aktörer inom området har den kompetens som efterfrågas. Vi har bland annat en dialog med MSB avseende kompetensförsörjning. (SOFF)

- Arrangerar nätverksträffar på löpande basis med aktörer från offentliga och privata organisationer för att ge möjlighet till kontaktskapande. På dessa träffar, som samlar mellan 40–60 personer, deltar centrala aktörer från våra företag och centrala aktörer från myndigheter samt politiker och Regeringskansliet. (SOFF)

- Sponsrar Cyber Challenge, en policyorienterad cybersäkerhetstävling för studenter som FHS anordnar på uppdrag av MSB. I år var sju av våra företag med som domare och finansiärer. (SOFF)

- Involverad i diskussion och utveckling av en cybernod och testanläggning (cyberrange) med forskningsinstitutet RISE. (TF)

- Involverad i prioritering av cybersäkerhetsforskning på RISE genom ICT Sweden samt med VINNOVA. (TF)

Vår önskelista på kort sikt (de första två åren från öppnandet)

Nedanstående förslag utgår från den gemensamma myndighetsrapporten och ovanstående lämnade synpunkter.

1. **I samverkan med näringslivet genomföra operativ koordinering vid allvarliga cyberattacker**
   Det mest grundläggande, och därmed kärnan i det arbete som centret ska bedriva, är att staten med kraft kan uppträda som en samlad aktör. För att detta arbete ska nå framgång är näringslivets deltagande avgörande. Givetvis kan all information inte alltid delges alla aktörer när något allvarligt händer. Men bara vetskapen om att det finns *en* aktör från staten som har ansvar och ambition att involvera näringslivet kommer att kunna förbättra hanteringen av framtida allvarliga cyberincidenter.

2. **I samverkan med näringslivet utbyta information kring hotbild, aktörer och attacker** Säkerställa tidskritisk och relevant informationsdelning mellan deltagande parter (Offentlig-Offentligt/Ofentligt-Privat/Nationell-Internationell). I detta ingår att lösa ut frågan om minutoperativ informationsdelning mellan myndigheterna som ingår i centret och till deltagande parter i näringslivet och att samtidigt upprätthålla sekretessen för såväl de offentliga som privata aktörerna som deltar i centrets arbete. För att skapa ett förtroendefullt forum krävs regelbundna fysiska möten och möjligheter för de centrala företag som förhoppningsvis kommer adjungeras till centret att ha en egen arbetsplats där. Informationen måste även kunna delas digitalt.

   Centret får inte bli ett ”svart hål” dit information förmedlas in och sedan stannar. Informationen måste förmedlas ut till näringsliv, kommuner, andra myndigheter och samhället i stort. Information behöver kunna delas på olika sekretessnivåer, annars kommer informationen inte att komma ut i organisationerna. Det är även viktigt att informationen är formulerad med en lingvistik anpassad efter mottagande part. En närliggande aspekt är därtill att utbilda mottagarna i hur informationen tolkas, hanteras och kan spridas. Det faktum att företag som har strategisk betydelse i Sverige, i varierande utsträckning, har utländska ägare, kommer också behöva adresseras och hanteras.

3. **I samverkan med näringslivet, arbeta fram och upprätthålla en nationell gemensam och samlad cyberlägesuppfattning** och förmedla denna till relevanta aktörer, båda i den offentliga sfären och i det privata näringslivet. Vi anser det bra och viktigt att regeringsbeslutet nämner att centret tillsammans med näringsliv kan göra gemensamma analyser och lägesbilder om hot, sårbarheter och risker inom cyberområdet. Vi vill framhålla att näringslivet kan bistå med god kunskap och unik förmåga.

4. **I samverkan med näringslivet, ta fram en nationell hanterings- och beredskapsplan för cyberområdet**

Det behövs en plan som visar på vad olika aktörer har för ansvar och vem som ansvarar för vad när något händer. En sådan plan fanns 2011 men har därefter inte reviderats.[3] Detta är en central åtgärd för att bringa ordning. Som det är nu så är kunskapen om vem som har vilket ansvar begränsat i samhället och hos våra företag. En sådan plan måste också kommuniceras ut till alla aktörer, i detta kan vi och våra företag vara behjälpliga.

Önskelista på lång sikt (Efter 2023)

Nedanstående förslag utgår från att allt inte kan göras de närmaste åren men att det finns ett antal frågor som vi ser att centret kan hantera efter några år när det är mer etablerat.

1. **Utifrån de första årens erfarenheter utvärdera cybersäkerhetscentret och där ingående aktörer i syfte att undersöka:**
   a. om strukturella/ organisatoriska förändringar behöver ske,
   b. om de ekonomiska medlen är tillräckliga och
   c. om de legala förutsättningarna till stöd för centret är tillräckliga.

2. **Utföra en strategisk analys av de legala förutsättningarna inom informations- och cybersäkerhetsområdet i ett helt digitaliserat samhälle**
   När det gäller de legala förutsättningarna finns det utöver de direkt legala förutsättningarna för centrets verksamhet flera särskilda överväganden som behöver ske. En hel del arbete har redan genomförts efter händelserna inom Transportstyrelsen, vissa av dessa åtgärder har varit absolut nödvändiga medan andra har haft väldigt långtgående effekter för olika företag. Här behöver en strategisk analys förslagsvis en utredning ske av hur vi ska se på informations- och cybersäkerhet i ett helt digitaliserat samhälle.

3. **Etablera sektorsvisa responsmiljöer, sektorsvisa CERT-funktioner i alla de samhällskritiska sektorerna såsom energi, finans, transport och hälso- och sjukvården i linje med vad som finns i Norge**
   I Norge finns det sektorsvisa CERT:ar inom finans, kraft (energi), hälsa och transporter. Det Norska Cybercentret (NCSC) bistår dessa sektors-CERT:ar och de bistår i sin tur aktörerna i sina sektorer. Nyttan med att ha specialiserade CERT- funktioner som kan arbeta nära det nationella cybercentret kan inte överskattas. Ju bättre kunskap och närhet som finns till en sektor desto snabbare och effektivare respons, speciellt i en situation där flera sektorer samtidigt blir drabbade.

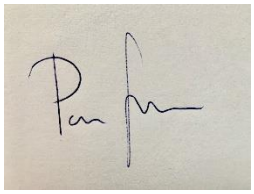
4. **Ta fram hanterings- och beredskapsplaner för cyber för alla samhällskritiska sektorer utifrån den nationella hanterings- och beredskapsplanen inom cyberområdet, som föreslås tas fram enligt ovan**
   På sikt räcker inte en övergripande nationell hanterings- och beredskapsplan inom cyberområdet. I ett helt digitaliserat samhälle finns ett stort behov av att även göra planer inom alla samhällskritiska sektorer, detta för att skapa

[3] Hantering av allvarliga IT-incidenter – Nationell hanterandeplan interimistisk version, mars 2011.

tydlighet avseende vad de offentliga aktörerna respektive de privata aktörerna gör. Om detta ska göras sektorsvis, eller på regional nivå (Regioner/Länsstyrelser) behöver närmare belysas.

Säkerhets- och försvarsföretagen och Teknikföretagen vill vara ett stöd och en förtroendefull partner vid skapandet av Sveriges nationella cybersäkerhetscenter.

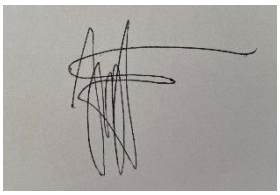
För Teknikföretagen,



Patrik Sandgren

Ansvarig för digitaliseringsfrågor

För Säkerhets- och försvarsföretagen,



Annika Avén

Ansvarig Cyberförsvar