INTERNET STIFTELSEN

2024-12-20

Försvarsdepartementet

Rättssekretariatet

Fö2024/01550

Internetstiftelsens remissvar på betänkandet Motståndskraft i samhällsviktiga tjänster (SOU 2024:64)

Stiftelsen för Internetinfrastruktur (”Internetstiftelsen”) är inte upptagna som remissinstans i denna remiss, vilket vi förmodar vara ett förbiseende då Internetstiftelsen direkt kan träffas av lagstiftningen såsom kritisk verksamhetsutövare.

Om Internetstiftelsen

Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkar för ett internet som bidrar positivt till människan och samhället.

Vi är en stiftelse och vår urkund slår fast att vi ska säkerställa en stark och säker infrastruktur för internet som tillgodoser dagens och framtidens behov i Sverige samt främja forskning, utbildning och undervisning med inriktning på internet. Vi ansvarar för internets svenska toppdomän .se och sköter även drift och administration av toppdomänen .nu. Intäkterna från affärsverksamheten finansierar en rad satsningar i syfte att möjliggöra att människor kan nyttja internet på bästa sätt och att ge kunskap om internetanvändningen i Sverige samt digitaliseringens påverkan på samhället. Vi tillhandahåller evenemang och utbildningsinsatser som gör det enklare att förstå och använda internets tjänster och som bidrar till ökad kompetens och fler möten som främjar internetinnovation. Vi stöttar även olika fristående uppdrags- och forskningsprojekt som på olika sätt gynnar internets utveckling och ger förutsättningar för internetentreprenörer och utvecklare att ta steget från idéstadie till färdig produkt eller tjänst. Med våra identitetsfederationer förenklar vi inloggning och höjer säkerheten i identitets- och kontohantering för både användare och leverantörer av olika tjänster inom skola, hälso- och sjukvård.

Vi tycker om och tror på internet och brinner för att dela med oss av vår kunskap. Vår vision är att alla i Sverige vill, vågar och kan använda internet.

Inledning

Cybersäkerhet och därtill motståndskraft hos verksamhetsutövare är angelägna frågor och Internetstiftelsen är positiv till ambitionen att uppnå en högre grad av harmonisering inom detta område.

Sammanfattning

Internetstiftelsen har inget att erinra mot förslaget att sådant som regleras i lagen om cybersäkerhet undantas i denna lag, samt inte heller någon erinran mot att undantag görs för verksamhetsutövare inom sektorerna bankverksamhet, finansmarknads-infrastruktur och digital infrastruktur.

Internetstiftelsen ställer sig positiv till att tillsynsmyndigheten ansvarar för identifieringen av kritiska verksamhetsutövare, men poängterar vikten av samstämmig tillsyn då en verksamhetsutövare kan bli föremål för tillsyn av flera tillsynsmyndigheter, men avseende olika samhällsviktiga tjänster.

Internetstiftelsen poängterar även att små aktörer kan identifieras som kritiska enligt förslaget vilket innebär ökade krav som dessa aktörer kan ha svårt att möta. Det kräver därmed särskilt stöd och vägledning från tillsynsmyndigheterna.

Internetstiftelsen stödjer förslaget att MSB ansvarar för en nationell, samlad förteckning som uppdateras regelbundet. MSB bör även ge stöd till tillsynsmyndigheter och samverka med EU för att säkerställa korrekt och effektiv rapportering.

Internetstiftelsen delar utredningens förslag om incidentrapportering, system för tillsyn och sekretessreglering.

Slutligen har Internetstiftelsen ett par redaktionella kommentarer.

Kommentarer på förslaget

5.3.1 Undantag för sådant som regleras i lagen om cybersäkerhet

Utredningens förslag är att lagen inte gäller för sådant som regleras i lagen om cybersäkerhet, vilket följer av direktivet.

Internetstiftelsen *har inget att erinra mot detta*, men föreslår att det kan behöva tydliggöras i föreskrifter vilka specifika delar som är reglerat i cybersäkerhetslagen, och därmed undantaget i lagen om motståndskraft i samhällsviktiga tjänster. Detta kan särskilt vara viktigt för mindre aktörer som inte har stora resurser för dessa legala bedömningar.

Utredningen föreslår under kapitel 5.3.3 att regeringen ger tillsynsmyndigheterna i uppdrag att utreda vilka kategorier av verksamhetsutövare inom respektive tillsynsområde som omfattas av annan lag eller andra bindande unionsrättsakter som innehåller bestämmelser med motsvarande verkan. I detta uppdrag skulle även kunna rymmas klargöranden vilka specifika skyldigheter som har företräde i cybersäkerhetslagen.

5.3.2 Undantag för verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur

Utredningen föreslår att för kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur gäller inte kapitel 3–6 i den föreslagna lagen. Innebörden blir då att vissa kritiska verksamhetsutövare kan identifieras som kritiska men ska endast omfattas av kapitel I, II (exkl. artikel 11) och V i CER-direktivet. Sammanfattningsvis konstateras att de artiklar som gäller för de aktuella verksamhetsutövarna medför rättigheter snarare än skyldigheter.

Denna paragraf blir direkt tillämplig på Internetstiftelsen och Internetstiftelsen *har inget att erinra mot* föreslagen reglering.

6.1 Nationell riskbedömning

Vad avser riskbedömningar vill Internetstiftelsen påtala följande.

Genom att tillgängliggöra den nationella riskbedömningen för kritiska verksamhetsutövare i landet kommer det att bidra till en ökad samsyn för vilka risker som identifierats och de utmaningar vi står inför. Det kommer bidra till att åtgärder implementeras för att stärka de kritiska verksamhetsutövares motståndskraft.

Då förslaget ser att även tillsynsmyndigheterna bör ges möjlighet att inhämta de uppgifter som behövs från kritiska verksamhetsutövare för att den nationella riskbedömningen ska kunna upprättas är det av stor vikt att ett verktyg med tillhörande processer och rutiner implementeras för att kunna säkerställa att känslig information i inhämtade uppgifter hanteras på ett likadant sätt som sekretessen för rapportering avseende incidenter.

6.3 Krav för identifiering av kritiska verksamhetsutövare

Internetstiftelsen ställer sig positiv till att tillsynsmyndigheten ansvarar för identifieringen av kritiska verksamhetsutövare. Det är också rimligt att denna myndighet beslutar om och kommunicerar vilka verksamhetsutövare som identifieras som kritiska baserat på riskbedömningen som ska användas av de behöriga myndigheterna vid identifiering av kritiska verksamhetsutövare, samt för att bistå de kritiska verksamhetsutövarna med att vidta åtgärder för motståndskraft.

Om en verksamhetsutövare tillhandahåller flera samhällsviktiga tjänster och där verksamhetsutövaren kan identifieras som kritisk av flera tillsynsmyndigheter är det därmed viktigt att tillsynen kan ske i så bred samstämmighet som möjligt och i dialog med de olika tillsynsmyndigheterna.

6.4 Betydande störande effekt

Enligt utredningens bedömning bör de tröskelvärden som ska tas fram för att fastställa när en störande effekt är betydande bestämmas till en sådan nivå att de fastställda tröskelvärdena inte medför att samtliga verksamhetsutövare som erbjuder en samhällsviktig tjänst identifieras som kritisk verksamhetsutövare. Tröskelvärdena riskerar att variera mellan sektorer och myndigheter, vilket kan leda till ojämlik tillämpning och rättsosäkerhet. Att små aktörer kan identifieras som kritiska enligt förslaget innebär även ökade krav som dessa aktörer kan ha svårt att möta.

Det kräver därmed särskilt stöd och vägledning från tillsynsmyndigheterna. Regeringen bör säkerställa att MSB och andra tillsynsmyndigheter utvecklar en tydlig vägledning för hur kriterierna ska tillämpas i praktiken.

6.5 Beslut om identifiering och underrättelse om skyldigheter

Förslaget att vissa verksamhetsutövare inom dessa sektorer undantas från delar av lagen om motståndskraft hos kritiska verksamhetsutövare är i linje med CER-direktivets intentioner.

Internetstiftelsen har inget att invända mot detta, men anser att beslut om undantag bör inkludera en tydlig motivering och referens till tillämpliga lagar och direktiv.

6.6 En kritisk verksamhetsutövare är en väsentlig verksamhetsutövare enligt cybersäkerhetslagen

Internetstiftelsen ställer sig bakom förslaget att verksamhetsutövare som identifieras som kritiska enligt lagen om motståndskraft hos kritiska verksamhetsutövare också bör

betraktas som väsentliga enligt cybersäkerhetslagen. Detta tydliggör ansvarsfördelningen och säkerställer enhetliga skyldigheter. Eftersom vissa verksamhetsutövare kan omfattas av CER-direktivet men inte av NIS2-direktivet, finns en risk för oklara ansvarsförhållanden. Det är viktigt att tydliga ansvarsområden definieras för att undvika duplicering av tillsyn och rapporteringskrav. Harmonisering mellan CER- och NIS2-direktivet är avgörande för att undvika konflikter och underlätta efterlevnad.

Vi noterar att detta kan innebära att mindre verksamheter utan storlekskrav omfattas av cybersäkerhetslagen. Tillsynsmyndigheten bör särskilt beaktar behovet av stöd och vägledning för dessa aktörer, i linje med utredningens förslag.

6.7 Förteckning och information till kommissionen

Utredningens förslag om att upprätta och samordna förteckningar över kritiska verksamhetsutövare och samhällsviktiga tjänster i enlighet med CER-direktivets krav innebär att frågan om sekretess för information som rör kritiska verksamhetsutövare är avgörande. Förslaget måste behandlas i särskild ordning och *Internetstiftelsen vill understryka vikten av skydd för känslig information*. Identiteten på kritiska verksamhetsutövare och deras sektorsspecifika roller är potentiellt säkerhetskänsliga. Regelverk för hantering av dessa uppgifter bör vara strikt och tydligt definierat. Det måste finnas en balans mellan insyn och säkerhet. Det är viktigt att uppnå en balans mellan att uppfylla kommissionens krav på information och att skydda nationella säkerhetsintressen.

Artikel 6.3 och artikel 7.2 har olika, men sammanhängande syften.

- Artikel 6.3: Fokuserar på nationellt identifierings- och underrättelsearbete. Medlemsstater ska upprätta en förteckning över identifierade kritiska entiteter och underrätta dessa om deras skyldigheter och tidsramar. Syftet är att säkerställa efterlevnad av skyldigheter på nationell nivå.
- Artikel 7.2: Handlar om rapportering till EU-kommissionen. Medlemsstater ska lämna aggregerad information om samhällsviktiga tjänster, kritiska entiteter och tröskelvärden. Syftet är att främja harmonisering och transparens på EU-nivå.

Internetstiftelsen anser att de olika syftena kräver tydligt separata vägledningar för att undvika förvirring och säkerställa att ansvariga myndigheter hanterar nationella och EU-relaterade krav korrekt. Specifikt behövs tydlig information till kritiska entiteter. Vägledningar bör beskriva hur tillsynsmyndigheter ska identifiera och informera kritiska entiteter om deras specifika skyldigheter och undantag och för EU-rapportering gällande aggregations- och rapporteringsmetoder för att möta EU-kraven bör vägledningar inkludera exempel på hur data kan sammanställas, anonymiseras och presenteras. Tydliga och särskiljande vägledningar är avgörande för att säkerställa att kraven i båda artiklarna efterlevs på ett effektivt och rättssäkert sätt.

Internetstiftelsen stödjer förslaget att MSB ansvarar för en nationell, samlad förteckning som uppdateras regelbundet. MSB bör även ge stöd till tillsynsmyndigheter och samverka med EU för att säkerställa korrekt och effektiv rapportering.

8.3 Incidentrapportering

Utredningen föreslår att incidentrapportering bör ske till MSB för att på så sätt hålla samman rapporteringen enligt de två direktiven. *Internetstiftelsen delar denna uppfattning.*

10.2 System för tillsyn

Utredningen föreslår att systemet för tillsyn för CER-direktivet följer den struktur som föreslås för NIS2-direktivets genomförande i Sverige. *Internetstiftelsen delar denna uppfattning.*

13 Sekretess
Frågan om sekretess för uppgifter som rör incidentrapportering, med mera

Utredningen föreslår att en ny sekretessbestämmelse bör införas i offentlighets- och sekretesslagen med syfte att ge skydd för uppgift i incidentrapporter samt uppgift om åtgärd som följer av en sådan incident.

Internetstiftelsen noterar att skrivningen avser ”uppgift i incidentrapporter” men inte uppgift *om vem* som lämnat in incidentrapporten. Beroende på kommande tekniska lösningar för incidentrapportering elektroniskt bör frågan lyftas om även *vem* som rapporterat omfattas av skrivningen i OSL.

Internetstiftelsen delar i övrigt utredningens bedömning att sekretessbestämmelsen bör utformas med ett omvänt skaderekvisit, med hänsyn till den skada som kan uppstå genom ett röjande av uppgifterna.

Redaktionella kommentarer
SOU sida 42
I föreslagen lag om motståndskraft hos kritiska verksamhetsutövare 2 kap. paragraf 3 görs en felhänvisning till lagen om cybersäkerhet. 2 kap. 1 § 8 finns inte i föreslagen cybersäkerhetslag.

SOU sida 80
1.10 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)

Notera att det anges att förordningen träder i kraft den 1 januari 2025 i fråga om lagen (2025:000) om cybersäkerhet och i övrigt den 1 augusti 2025. Datumet 1 januari 2025 bör justeras med hänsyn till cybersäkerhetslagens senarelagda ikraftträdande.

Ärendet har beretts av senior legal counsel Filippa Murath och Chief Information Security Officer Catharina Ankre.

För Internetstiftelsen

Carl Piva