TechSverige

Datum
2026-11-09

Vår referens

RL

Justitiedepartementet

ju.remissvar@regeringskansliet.se

Kopia till
ju.L4@regeringskansliet.se

Remissvar avseende betänkandet Effektiva ingripanden mot brott i cybermiljö (SOU 2026:45)

TechSverige har givits möjlighet att yttra sig över betänkandet Effektiva ingripanden mot brott i cybermiljö (SOU 2026:45).

TechSverige är den ledande bransch- och arbetsgivarorganisation som samlar kärnan av svensk tech – företag som utvecklar, levererar och möjliggör tech i Sverige och som verkar på den svenska, europeiska och globala marknaden. Vi företräder cirka 1 400 företag som sammantaget har närmare 100 000 medarbetare i Sverige.

TechSveriges uppdrag är att tillsammans med våra medlemmar skapa goda villkor för en konkurrenskraftig och ansvarstagande techbransch i Sverige.

Inledning och samlad bedömning

Digitala tjänster och digital infrastruktur bär i dag stora delar av samhället. När dessa miljöer utnyttjas för brott påverkas människors trygghet, företagens verksamhet och tilliten till det digitala samhället.

Samhällets förmåga att förebygga och bekämpa cyberbrott behöver därför stärkas. I framtidsagendan Techsäkra Sverige efterfrågar TechSverige fler cyberpoliser och riktade resurser för stärkt cyberkompetens inom brottsbekämpande och rättsvårdande myndigheter. Ändamålsenliga rättsliga verktyg är också en viktig del av denna förmåga.

TechSverige stödjer inriktningen att stärka möjligheterna att förebygga och bekämpa brott i cybermiljö. Samtidigt kan ingripanden beröra nät, system och tjänster som används för legitim och samhällsviktig verksamhet. Regleringen behöver därför bidra både till en effektiv brottsbekämpning och till säkra och motståndskraftiga digitala miljöer, med respekt för den personliga integriteten och med bibehållet förtroende för digitala tjänster.

TechSverige välkomnar att förslaget inte innebär någon generell anpassnings- eller lagringsskyldighet, att kostnader för medverkan ska ersättas samt att lagen föreslås vara tidsbegränsad och utvärderas. Företagens medverkan kan bidra till effektiva, precisa och säkra ingripanden. Skyldigheterna behöver vara tydligt avgränsade till medverkan i

enskilda ärenden med tillgängliga uppgifter, funktioner och tekniska metoder samt förenade med ersättning och en klar ansvarsfördelning.

TechSverige bedömer samtidigt att förslaget behöver bearbetas ytterligare innan det läggs till grund för lagstiftning. Medverkansmodellen behöver bygga på en samlad analys av faktisk teknisk rådighet, precision, säkerhetsrisker och kostnader. Beslutsordningen och rättssäkerhetsgarantierna behöver stärkas med hänsyn till ingripandenas möjliga konsekvenser, särskilt för företag som inte är misstänkta för brott och för deras användare. Företagens säkerhetsarbete, behov av information och möjligheter till samordning behöver beaktas och ges uttryckligt stöd i lagen.

Beslutsunderlaget behöver också kompletteras med en analys av konsekvenserna för berörda företag och andra användare, inklusive hur regleringen kan påverka konkurrenskraft och investeringar i digital infrastruktur och tjänster. De rättsliga förutsättningarna för gränsöverskridande ingripanden och frågor om ansvar och ersättning behöver klarläggas.

Nya befogenheter kräver ett brett beslutsunderlag

Förslaget ger brottsbekämpande myndigheter uttryckliga befogenheter att vidta åtgärder som annars kan omfattas av straffbestämmelsen om dataintrång. Det handlar bland annat om att bereda sig tillgång till informationssystem samt ändra, blockera eller radera uppgifter. Förslaget innebär därmed ett betydande steg i statens möjligheter att ingripa i den digitala miljön.

Utredningens internationella utblick visar att det finns utländska regler om åtkomst till informationssystem och i vissa fall om blockering eller nedstängning. De flesta jämförelser gäller dock befogenheter som närmast motsvarar genomsökning på distans eller hemlig dataavläsning. Det finns därmed begränsad jämförbar praktisk erfarenhet av en reglering med hela den bredd av ingripanden som nu föreslås.

Detta innebär inte att Sverige bör avstå från att utveckla nya verktyg. Det innebär däremot att kraven på analys blir särskilt höga. Den fortsatta beredningen behöver pröva olika sätt att uppnå syftet och bedöma deras effektivitet, tekniska genomförbarhet, inverkan på säkerheten i systemen och påverkan på andra verksamheter.

Gränsöverskridande ingripanden

För tjänster och informationssystem med gränsöverskridande kopplingar behöver den fortsatta beredningen klarlägga de rättsliga förutsättningarna för svensk verkställighet, särskilt när åtgärder berör system eller uppgifter i andra stater. Analysen behöver skilja mellan tillgång till uppgifter och åtgärder som ändrar, blockerar eller raderar dem, även när lagringsplatsen är okänd eller systemen är distribuerade över flera stater. Det behöver också klargöras hur befogenheterna förhåller sig till relevanta EU-regelverk och vilka former av internationellt rättsligt samarbete som kan användas för respektive åtgärd. För att kunna hantera gränsöverskridande rättsliga konflikter och bindande skyldigheter enligt utländsk lag behöver företagen kunna anlita juridiskt biträde och tillvarata sina möjligheter till rättslig prövning. Regleringen behöver uttryckligen säkerställa att företagen får lämna ut en begäran om medverkan, tillhörande beslut och nödvändiga uppgifter till juridiska ombud och behörig domstol även när uppgifterna omfattas av tystnadsplikt. Det behöver också klargöras under vilka förutsättningar beslut och nödvändiga uppgifter får lämnas till behöriga utländska tillsynsmyndigheter för att hantera sådana konflikter. Företagen behöver kunna förutse vilka krav som kan ställas och hur påtalade konflikter med andra rättsliga skyldigheter ska bedömas och hanteras.

Tydliga förutsättningar för gränsöverskridande ingripanden är viktiga både för en effektiv brottsbekämpning och för företagens möjligheter att agera rättssäkert.

Den fortsatta beredningen bör också beakta målet om en väl fungerande digital inre marknad i EU. Risken för nationella särkrav som skapar motstridiga skyldigheter eller onödiga hinder för digitala tjänster bör analyseras särskilt.

Medverkansmodellen behöver bygga på en samlad analys

Förslaget innebär att den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lagen om elektronisk kommunikation ska vara skyldig att medverka. Digitala tjänster består ofta av flera tekniska lager och aktörer. Olika aktörer kan därför ha olika faktisk rådighet och tekniska förutsättningar att medverka vid en viss åtgärd.

Utredningen redovisar att frågan om medverkan från aktörer som inte omfattas av den föreslagna bestämmelsen har väckts, men bedömer att en utvidgad medverkansskyldighet ligger utanför direktiven och är alltför komplex för att behandlas inom utredningen. Betänkandet innehåller inte någon samlad analys av olika aktörers faktiska förutsättningar att medverka.

TechSverige tar inte ställning till vilka aktörer som slutligen bör omfattas av en medverkansskyldighet. Den fortsatta beredningen behöver kompletteras med en samlad analys av olika aktörers faktiska förutsättningar att medverka. En eventuell utvidgning av medverkansskyldigheten till ytterligare kategorier av aktörer, exempelvis tillhandahållare av nummeroberoende interpersonella kommunikationstjänster, molntjänster eller lagringstjänster, måste dock föregås av en separat remissbehandling och en fullständig konsekvensanalys samt förenas med motsvarande rättssäkerhetsgarantier. En sådan analys bör pröva vilken ansvarsfördelning och medverkansmodell som, utifrån faktisk teknisk rådighet, precision, säkerhetsrisker och kostnader, ger bäst brottsbekämpande effekt med minst påverkan på andra användare och legitim verksamhet. Analysen bör skilja mellan att lämna befintliga upplysningar och att aktivt medverka vid en teknisk åtgärd samt beakta förutsättningarna för olika åtgärder och tekniska lager.

Kravet på att välja den minst ingripande åtgärden i ett enskilt ärende är viktigt. Det kan dock inte ersätta lagstiftarens ansvar att, innan medverkansmodellen fastställs, bedöma om den övergripande regleringsmodellen ger bästa möjliga effekt med minsta möjliga påverkan.

Medverkansskyldigheten behöver få tydliga gränser

TechSverige välkomnar att förslaget inte innebär någon generell anpassnings- eller lagringsskyldighet. Medverkan i ett enskilt ärende kan samtidigt kräva aktivt tekniskt arbete. Medverkansskyldigheten bör vara begränsad till uppgifter, funktioner och tekniska metoder som företaget redan förfogar över, inom ramen för ett konkret beslut om ingripande.

Medverkansskyldigheten bör inte innebära krav på att utveckla, anskaffa eller permanent installera ny funktionalitet eller genomföra systemförändringar som skapar nya förmågor för ingripanden. Den bör inte heller innebära krav på att hålla särskilda personella eller tekniska resurser i beredskap för eventuella framtida ingripanden. Möjligheten att utveckla eller köpa in en teknisk lösning innebär inte att lösningen redan är tillgänglig.

Vilka konkreta insatser som en operatör ska bistå med kommer enligt författningskommentaren att bero på hur myndigheten formulerar sin begäran. Det ger

utrymme för att beakta förutsättningarna i det enskilda fallet, men skapar också behov av tydliga yttre gränser för vad som kan krävas.

Gränsen mellan medverkan och anpassning behöver framgå tydligt av regleringen och upprätthållas vid tillämpningen. Enskilda eller återkommande myndighetsbegäranden ska inte medföra att företagen i praktiken åläggs en anpassningsskyldighet. Kraven behöver också hålla sig inom företagets faktiska tekniska och rättsliga rådighet. Medverkansskyldighetens grundläggande avgränsning behöver framgå direkt av lagen och får inte vidgas genom föreskrifter om hur medverkan ska genomföras.

Rättsliga skyldigheter och hantering av medverkansbegäranden

Utredningen föreslår ändringar i lagen om elektronisk kommunikation för att möjliggöra viss behandling och visst utlämnande av uppgifter samt utvidga tystnadsplikten till att omfatta uppgifter om en begäran om medverkan. Den fortsatta beredningen behöver klargöra hur medverkanskrav förhåller sig till företagens övriga rättsliga skyldigheter, bland annat att skydda kommunikation och personuppgifter, bevara vissa uppgifter och rapportera säkerhetsincidenter. Det gäller bland annat hur tystnadsplikt och andra begränsningar av informationslämnande förhåller sig till tillämpliga skyldigheter enligt GDPR och DSA, exempelvis att informera registrerade vid personuppgiftsincidenter och att lämna information eller motiveringar till användare när innehåll eller tjänster begränsas. Om medverkan förutsätter ytterligare undantag från sådana skyldigheter behöver dessa ha ett tydligt och preciserat stöd i lag. Eventuella begränsningar av informationsskyldigheten enligt artikel 34 GDPR behöver uppfylla förutsättningarna i artikel 23, bland annat kraven på nödvändighet och proportionalitet. Företagen ska kunna följa en begäran utan osäkerhet om vilka rättsliga krav som gäller.

En begäran om medverkan behöver vara tillräckligt konkret för att företaget ska kunna bedöma dess tekniska förutsättningar och påtala eventuella hinder eller säkerhetsrisker. Medverkansbegäranden behöver förmedlas genom säkra och verifierbara kontaktvägar, med utgångspunkt i etablerade rutiner mellan myndigheter och företag. Företaget behöver kunna verifiera begärans äkthet, avsändarens behörighet och att begäran överensstämmer med myndighetens beslut. Det behöver klargöras hur företagens invändningar ska hanteras och vilka möjligheter som finns till skyndsam omprövning, särskilt när företaget identifierar risk för allvarliga eller svåråterkalleliga följder. Myndigheten ska ansvara för den rättsliga bedömningen och beslutet att ingripa.

Driftsäkerhet och ansvar behöver säkerställas

Eftersom nät, servrar och tjänster kan delas av flera kunder kan ett ingripande få konsekvenser även utanför det direkta målet. Kravet på att begränsa påverkan på andra behöver därför tillämpas med hänsyn även till beroende system, legitim verksamhet och samhällsviktiga tjänster. I tjänster som delas av många kunder bör ett ingripande så långt möjligt riktas mot ett enskilt användarkonto snarare än mot delade servrar eller delad infrastruktur. Även vid åtgärder mot ett enskilt konto behöver beroenden och möjliga följdverkningar bedömas. Samordning med verksamhetsutövaren och en tydlig teknisk avgränsning är viktiga för att begränsa påverkan på laglig kommunikation och andra användares legitima användning.

Ingripanden bör genomföras så att risken för driftstörningar, dataförlust och andra följdskador minimeras. Myndigheterna behöver ha tillräcklig teknisk kompetens och tydliga rutiner för riskbedömning före ingripandet och skadebegränsning under genomförandet. Rutinerna behöver också omfatta hur ingripandet kan avbrytas eller justeras om oväntade risker eller följdverkningar uppstår. Åtgärderna ska inte leda till en

generell försvagning av kryptering eller säkerheten i produkter och tjänster. Sårbarheter som myndigheterna identifierar eller utnyttjar bör som huvudregel rapporteras till berörd leverantör så att de kan åtgärdas, och det bör finnas en tydlig och transparent process för att avgöra när undantag får göras. Rapportering av sårbarheter bör ske samordnat och genom säkra kanaler så att risken för att känsliga uppgifter sprids till obehöriga begränsas. Berörd tillverkare eller utvecklare bör som huvudregel kontaktas direkt för att kunna åtgärda sårbarheten, vid behov med stöd av berörd CSIRT.

Att kringgå systemskydd, utnyttja sårbarheter eller installera tekniska hjälpmedel kan medföra säkerhetsrisker även efter att ingripandet har avslutats. Förslaget innehåller krav på att installerade tekniska hjälpmedel ska tas bort eller göras obrukbara. Detta behöver kompletteras med tydliga rutiner för dokumentation, hantering av kvarstående säkerhetsrisker, återställande och efterkontroll tillsammans med berörd verksamhetsutövare. Återställandet bör avse förändringar och säkerhetsrisker som inte behöver kvarstå för att upprätthålla ingripandets avsedda och lagligen beslutade verkan. Vid åtgärder i driftskritiska eller säkerhetskänsliga miljöer behöver också formerna för samordning klargöras, med beaktande av både ingripandets syfte och verksamhetens säkerhetskrav.

Ansvar vid skador och driftstörningar

Utredningen bedömer att befintliga skadeståndsregler är tillräckliga. Ansvarsfördelningen vid skador och driftstörningar behöver klargöras i den fortsatta beredningen. Ett företag som medverkar, eller vars system eller tjänster berörs av ett ingripande, bör inte behöva bära ansvar för följder av en myndighetsbeslutad åtgärd som företaget inte har kunnat påverka, och bör inte heller kunna hållas ansvarigt gentemot sina egna kunder för sådana följder. Regleringen behöver innehålla ett uttryckligt skydd mot civilrättsligt ansvar gentemot kunder och andra tredje män, inklusive avtalsrättsliga anspråk, för följder av att företaget korrekt fullgör sin medverkansskyldighet vid myndighetsbeslutade åtgärder. Ansvarsreglernas räckvidd vid gränsöverskridande ingripanden behöver också belysas. Det behöver även klargöras hur skador för kunder och andra berörda ska hanteras. Analysen behöver även omfatta skador och avtalsrättsliga anspråk som kan uppkomma vid ett lagenligt ingripande.

Ingripanden i system hos företag som inte är misstänkta för brott kräver starkare rättssäkerhetsgarantier

Förslaget ger myndigheterna möjlighet att bereda sig tillgång till informationssystem, kringgå skydd, utnyttja tekniska sårbarheter och installera tekniska hjälpmedel samt att ändra, blockera och i undantagsfall radera uppgifter (3, 5, 9 och 17 §§ i den föreslagna lagen). Myndigheterna förväntas normalt själva bereda sig tillgång, och förslaget innehåller inget krav på att den verksamhetsutövare som tillhandahåller systemet eller tjänsten ska informeras inför ingripandet. I många fall saknar verksamhetsutövaren av en kommunikations-, lagrings- eller molntjänst helt koppling till den brottsliga verksamheten. Sådana åtgärder kan få mer långtgående verkningar än enbart inhämtning av uppgifter, eftersom de också kan ändra, blockera eller radera uppgifter i system som används av många andra. Att befogenheterna kan användas redan på underrättelsestadiet, och i vissa avseenden vid en låg tröskel, förstärker behovet av tydliga rättssäkerhetsgarantier.

Trafikkartläggning

Förslaget omfattar även tillfällig tillgång till trafikuppgifter för att kartlägga kommunikation mellan informationssystem. För denna befogenhet behöver det tydliggöras hur kartläggningens omfattning och varaktighet avgränsas, även vid

återkommande ingripanden, och hur andra användares kommunikation skyddas. Företagens medverkan behöver även här begränsas till befintliga uppgifter, funktioner och tekniska metoder.

Domstolsprövning och samordning

TechSverige anser att myndighetsåtgärder som innebär åtkomst till eller påverkan på informationssystem eller tjänster vars ägare eller verksamhetsutövare inte misstänks för inblandning i den brottsliga verksamheten som huvudregel bör kräva domstolstillstånd. Åtgärderna kan få betydande konsekvenser för verksamhetsutövaren och dess kunder, vilket motiverar oberoende förhandsprövning. Tillstånd bör endast meddelas om syftet inte rimligen kan uppnås genom mindre ingripande åtgärder med tillräcklig effekt inom den tid som situationen kräver. Möjligheten till samordning med ägaren eller verksamhetsutövaren behöver bedömas inför beslut och genomförande, när sådan samordning är praktiskt möjlig och kan ske utan att ingripandets syfte äventyras. Undantag från kravet på domstolstillstånd i förväg bör vara snävt reglerade och förutsätta en konkret och omedelbar risk för allvarlig skada vid dröjsmål som inte kan hanteras genom mindre ingripande åtgärder. Sådana beslut ska skyndsamt underställas domstol inom en kort, lagbestämd frist. Åtgärder som innebär att uppgifter ändras, blockeras eller raderas behöver omgärdas av rättssäkerhetsgarantier som motsvarar deras faktiska verkningar. Samordning med verksamhetsutövaren ersätter inte kraven på rättsligt stöd och prövning när myndigheten använder de föreslagna befogenheterna.

Verksamhetsutövare övervakar kontinuerligt sina system för att upptäcka och stoppa intrång. Ett ingripande som verksamhetsutövaren inte känner till riskerar att upptäckas och motverkas av verksamhetsutövarens säkerhetsfunktioner, till exempel genom att åtkomst blockeras eller ändrade inloggningsuppgifter återställs. Det behöver klargöras hur ingripanden ska förhålla sig till verksamhetsutövarens ordinarie säkerhetsarbete och hur konflikter mellan åtgärderna ska hanteras. Det bör tydliggöras att en verksamhetsutövare som inom ramen för sitt ordinarie säkerhetsarbete upptäcker och motverkar ett ingripande som den inte har informerats om inte ådrar sig något ansvar, och att verksamhetsutövare inte är skyldiga att anpassa eller försvaga sina säkerhetsfunktioner med hänsyn till eventuella ingripanden. Det uttryckliga skyddet mot ansvar behöver även omfatta civilrättsliga och avtalsrättsliga anspråk som grundas på att företagets ordinarie automatiserade säkerhetsfunktioner, exempelvis DDoS-skydd eller filtrering av skadlig kod, motverkar ett myndighetsingripande som företaget inte har informerats om. Även när företaget har informerats behöver det klargöras hur ansvarsskyddet ska tillämpas om säkerhetsfunktionerna inte kan skilja myndighetens åtgärder från andra angrepp eller inte kan justeras utan att säkerheten försvagas. Samordning med verksamhetsutövaren skulle också minska risken för driftstörningar, dataförlust och motverkande åtgärder.

Radering av uppgifter

Radering av uppgifter kan vara oåterkallelig och är en av de mest ingripande åtgärderna i förslaget. Som huvudregel krävs beslut av åklagare, men i brådskande fall kan beslut fattas inom den ingripande myndigheten och därefter prövas av åklagare. Någon särskild ordning för överklagande till domstol föreslås inte. I moln- och kommunikationstjänster kan radering dessutom påverka säkerhetskopior, uppgifternas integritet samt verksamhetsutövares och deras kunders skyldigheter att bevara information. TechSverige anser att radering som huvudregel bör kräva domstolstillstånd i förväg. Ett brådskande undantag bör endast få användas under de snäva förutsättningar som anges ovan och när mindre ingripande alternativ, såsom tillfällig blockering eller isolering, inte är tillräckliga. Även i dessa fall ska beslutet skyndsamt underställas domstol.

Rättslig prövning och underrättelse

Dokumentation och tillsyn i efterhand är viktiga, men kan inte i sig förhindra att en irreversibel skada uppstår. Företag och andra berörda behöver också ha tydliga möjligheter att få omfattningen av krav och ingripanden rättsligt prövade. Operatörer och andra berörda verksamhetsutövare bör ges möjlighet att framföra tekniska och säkerhetsrelaterade invändningar och få dem prövade av ett oberoende organ, särskilt vid ingripanden som riktas mot infrastruktur och vid radering.

Den föreslagna underrättelseskyldigheten vid radering samt vid blockering som varat längre än en månad behöver kompletteras för tjänster som delas av många kunder. Förhållandet mellan underrättelse till berörd kund och till den ansvariga verksamhetsutövaren behöver klargöras. Verksamhetsutövaren bör som huvudregel underrättas innan ett ingripande genomförs i dess system eller infrastruktur, även när åtgärden avser en kunds uppgifter. Informationen behövs för att hantera säkerhetsrisker, följdverkningar och frågor från kunder. Informationen behöver också ge verksamhetsutövaren förutsättningar att dokumentera följderna och tillvarata sina möjligheter till rättslig prövning och ersättning.

Undantag från denna huvudregel behöver vara snävt avgränsade och bygga på konkreta skäl, exempelvis en påtaglig risk för att ingripandets syfte äventyras. Ett uppskov bör motiveras, dokumenteras och omfattas av oberoende kontroll samt följas av underrättelse så snart hindret har upphört. Behovet av att skydda tekniska metoder bör i första hand hanteras genom att begränsa informationens innehåll och kretsen av mottagare hos verksamhetsutövaren, i stället för att helt underlåta underrättelse.

Eventuella sanktioner

TechSverige anser att eventuella förslag om sanktioner för bristande medverkan behöver föregås av en särskild konsekvensanalys och kompletterande remissbehandling innan de läggs fram för riksdagen. Analysen behöver beakta medverkansskyldighetens avgränsning, företagens tekniska och rättsliga möjligheter att följa en begäran samt sanktionernas proportionalitet.

Ersättningsordningen behöver vara tydlig

TechSverige välkomnar att den ingripande myndigheten ska ersätta kostnader som uppstår vid medverkan. Ersättningen bör omfatta nödvändiga och skäliga merkostnader för den medverkan som begärs, exempelvis för personal, externa specialister, tekniska tester, säkerhetsåtgärder, återställande, incidenthantering och hantering av kund- och tredjemansanspråk. Vid utformningen av ersättningsordningen behöver det också beaktas att medverkan kan kräva att resurser tas från den ordinarie verksamheten.

Ersättningsreglerna behöver vara förenliga med medverkansskyldighetens avgränsning. Företagen ska inte hamna i en situation där myndigheten kräver insatser inom ramen för medverkansskyldigheten, samtidigt som kostnaderna bedöms avse generella systemanpassningar och därför inte ersätts.

Vilka kostnader som omfattas, hur ersättningen bestäms och hur eventuella tvister hanteras behöver klargöras innan regleringen börjar tillämpas. Utredningen anger att kostnader för medverkan kan ersättas även när ingripandet inte har kunnat genomföras.

Konsekvensanalysen behöver kompletteras före införandet

Konsekvensanalysen fokuserar på myndigheternas kostnader och förutsättningar att bygga upp den nya verksamheten. Däremot saknas en särskild analys av vad den

föreslagna medverkansskyldigheten innebär för berörda företag. Det behöver bland annat belysas vilka arbetsinsatser som kan krävas, vilka kostnader som kan uppstå och hur medverkan kan påverka bemanning, säkerhet och ordinarie verksamhet. Att kostnader för medverkan ska ersättas undanröjer inte behovet av en sådan analys.

Konsekvensanalysen behöver även belysa hur regleringen påverkar svensk konkurrenskraft och viljan att investera i digital infrastruktur och tjänster i Sverige. Förutsebara skyldigheter, tydliga ansvarsgränser och ett bibehållet förtroende för tjänsternas säkerhet är centrala för företagens långsiktiga investeringsbeslut.

Företagen kan också gynnas av effektivare ingripanden som minskar deras utsatthet för cyberbrott och motverkar att deras tjänster och infrastruktur utnyttjas för brott. Analysen behöver också omfatta hur ingripanden kan påverka samhällsviktiga tjänster, andra legitima användare och tilliten till digitala tjänster. Den bör genomföras i dialog med berörda företag och omfatta konkreta tekniska scenarier som belyser såväl avsedd effekt som möjliga följdverkningar. Dessa konsekvenser behöver vägas samman med den samhällsnytta som en effektivare brottsbekämpning kan ge. Analysen behöver även belysa konsekvenserna för företag vars system eller tjänster berörs utan att företaget självt medverkar, inklusive risken för konflikter med det ordinarie säkerhetsarbetet och rättsliga skyldigheter i andra länder. För företag som verkar i flera länder behöver analysen också belysa den samlade belastningen och risken för motstridiga krav om liknande nationella befogenheter införs med olika avgränsningar och förfaranden.

De berörda myndigheterna uppskattar att verksamheten, när den är uppbyggd, totalt kommer att omfatta minst 500 ärenden per år. Företagens faktiska belastning kommer emellertid att bero på hur ärendena fördelas, vilken teknisk komplexitet de har och vilka typer av insatser som begärs.

Uppföljning och utvärdering

TechSverige välkomnar att lagen föreslås bli tidsbegränsad och utvärderas innan en permanent reglering övervägs. Eftersom verksamheten förväntas byggas upp under nästan hela lagens femåriga giltighetstid behöver uppföljningen planeras och påbörjas redan när lagen träder i kraft. Den bör belysa både den brottsbekämpande effekten och konsekvenserna för företag, digital infrastruktur och andra användare. Erfarenheter av medverkanskrav, säkerhetsincidenter, kostnader och rättsliga invändningar behöver kunna tas till vara i utvärderingen. Den brottsbekämpande effekten bör bedömas utifrån om ingripandena leder till en varaktig minskning av brottsligheten och utsattheten för brott, om brottsligheten flyttas till andra tjänster eller jurisdiktioner och om samma resultat hade kunnat uppnås med mindre ingripande åtgärder. Antalet ärenden eller tekniskt genomförda ingripanden är inte i sig tillräckliga mått på effekt.

Avslutande synpunkter

TechSverige stödjer ambitionen att stärka brottsbekämpningen i cybermiljö. Den fortsatta beredningen behöver, i dialog med berörda företag, komplettera beslutsunderlaget och bearbeta förslaget i de avseenden som redovisats ovan.

Innan medverkansmodellen fastställs behövs en samlad analys av olika aktörers faktiska förutsättningar att medverka. Tydligt avgränsade skyldigheter, stärkta rättssäkerhetsgarantier samt en ändamålsenlig ansvars- och ersättningsordning är

centrala för att förena effektiv brottsbekämpning med en säker och förutsebar tillämpning.

För TechSverige

Christina Ramm-Ericson
näringspolitisk chef

Robert Liljeström
näringspolitisk expert