INTERNET STIFTELSEN

2026-02-27

policyomraden@mcf.se

Internetstiftelsens synpunkter på Riktlinjer/policyer till Sveriges nationella cybersäkerhetsstrategi

Om Internetstiftelsen

Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkarför 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. Internetstiftelsens största satsning, som finansierats med intäkter från domännamnsverksamheten, har varit att ta ansvar för att finansiera, etablera och utveckla en identitets- och behörighetsfederation för skol- samt vård- och omsorgssektorn. Med våra federationer; Sambi och Skolfederation, förenklar vi inloggning och höjer säkerheten i identitets- och kontohantering för både användare och leverantörer.

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.

Stärkt säkerhet i digitala leveranskedjor (7.2 a)

Internetstiftelsen delar bedömningen att digitala leveranskedjor präglas av hög komplexitet, tjänstekoncentration och begränsad insyn, vilket innebär att incidenter hos enskilda leverantörer kan få bred samhällspåverkan. Vi instämmer även i att den ökade mängden reglering på området bidrar till att stärka cybersäkerheten, men vill särskilt betona konsekvenserna för små och medelstora företag (SMF).

Regleringsbördan riskerar att minska faktisk regelefterlevnad hos SMF

Internetstiftelsen vill framhålla att den samlade mängden EU-regelverk på cybersäkerhetsområdet innebär en betydande administrativ och ekonomisk belastning för små och medelstora företag. Även när viljan att göra rätt är hög saknas ofta praktiska förutsättningar att fullt ut leva upp till kraven, exempelvis på grund av begränsade personella resurser, kompetens och budget. Detta riskerar att leda till ojämn regelefterlevnad och i förlängningen att regleringen får svagare faktisk effekt än avsett.

Ökad regelbörda kan även riskera att leda till ökad inlåsningseffekt och/eller monoberoende utifrån att företagen behöver välja en lösning som påstår sig uppfylla kraven.

Behov av konkret vägledning och operativt stöd

För att lagstiftning och styrning ska bli verkningsfull krävs att de aktörer som förväntas följa regelverken får tillgång till begriplig och tillämpbar vägledning. Internetstiftelsen ser en utmaning i att kraven ofta är spridda över flera regelverk och att det saknas tillräckligt sammanhållna råd, metodstöd och praktiska verktyg, särskilt riktade till mindre aktörer. Vägledning behöver vara handfast och utformad så att den kan användas utan omfattande juridisk och teknisk specialkompetens.

Staten behöver avsätta resurser för att stödet ska fungera i praktiken

Internetstiftelsen menar att det inte är realistiskt att förvänta sig att SMF själva ska bära hela kostnaden för att tolka, implementera och löpande efterleva en snabbt växande och komplex cybersäkerhetsreglering. För att uppnå avsedd samhällseffekt behöver staten avsätta resurser för rådgivning, utbildningsinsatser och tillämpningsstöd. Det kan exempelvis handla om skalbara stödfunktioner, mallar och kravpaket, branschspecifika exempel samt tillgängliga kontaktvägar för löpande frågor.

Vi finner det positivt att Metodstödet ska uppdateras och utvecklas för systematiskt cybersäkerhetsarbete så att det finns stöd till verksamhetsutövare.

Det är även positivt att tjänsten Cybersäkerhetsrådgivningen ska utvecklas och det ska tillsättas resurser för denna.

Mätbara mål för uppföljning och utvärdering

Policyn inför termen *monoberoende* i listan över definitioner men är inget som finns definierat i MCF:s termbank. Dock definierar de inte tydliga tröskelvärden, för hur många leverantörer som krävs för att ett beroende inte längre ska klassas som det. Detta är något som ofta diskuteras vid granskningar och avtalsskrivningar.

Gällande målet att “Vid slutet av år 2029 har mindre än 20 digitala leveranskedjeincidenter där 20 eller fler mottagare har drabbats inträffat under det senaste året.” är svårbedömt. Det är ett svårt mål att sätta i relation till nuläget som

MCF nämner i nulägesanalysen. Förslagsvis kan processuella mål istället formuleras utifrån nuläge.

Policyn nämner även “...stoppa eller begränsa s.k. högriskleverantörers verksamhet...” inte heller här finns det någon tydlig definition eller vilka kriterier som ska användas för identifiering av sådana eller uppföljning. Frågan är hur detta ska mätas långsiktigt.

Policyn anger flera åtgärder men saknar en tydlig plan för hur resultaten ska mätas och utvärderas. Till exempel den första åtgärden som regeringen rekommenderar att vidta, att NCSC ska kontinuerligt samla in uppgifter från verksamhetsutövare om deras digitala leveranskedjor för att därigenom möjliggöra ett effektivt genomförande av det nationella cybersäkerhetscentrets åtgärd nr. 6 kartlägga leveranskedjor. Dock anges det inte hur data ska användas för att bedöma effektiviteten av policyn. Det blir även problematiskt när rekommendationen för verksamhetsutövare som omfattas av Cybersäkerhetslagen och verksamhetsutövare som är leverantörer av digitala produkter bör använda tjänsten Cybersäkerhetskollen. För att säkerställa att målen satta i policyn blir genomförda bör varje åtgärd kopplas till mätbara resultat och tidslinjer.

Den föreslagna målbilden för 2029 och de listade åtgärderna pekar mot ett mer systematiskt och transparent arbetssätt. Samtidigt skulle policyn vinna på att konkretisera vissa begrepp, definiera mätbara mål och tydligt beskriva hur små och medelstora verksamheter ska få stöd. Ökad klarhet kring datahantering, riskhantering och tekniska säkerhetsåtgärder skulle stärka policyns genomförbarhet och bidra till att svenska organisationer i större utsträckning kan omsätta den i praktiken.

Frågan om uppföljning och utvärdering är generellt en kommentar som berör flera av policyerna.

Proportionalitet och genomförbarhet som styrande princip

Internetstiftelsen vill slutligen understryka vikten av att proportionalitet och genomförbarhet vägs in i fortsatt utveckling av föreskrifter, tillsyn och stödmaterial. Ett regelverk som upplevs som övermäktigt riskerar att skapa ett “compliance-gap” där särskilt mindre aktörer hamnar utanför, vilket i sig kan öka sårbarheten i digitala leveranskedjor.

7.2c Policy för hantering av sårbarheter och sårbarhetsinformation

Behov av konkret vägledning och operativt stöd kring sårbarhetshantering och CVD-processen

Det finns ett stort behov av handfast, sammanhållen vägledning och praktiska verktyg som kan omsättas i verksamheten utan omfattande juridisk eller teknisk specialkompetens. Kraven på att rapportera aktivt utnyttjade sårbarheter till nationell CSIRT inom 24 timmar och att kunna leverera Software Bill of Materials (SBOM) från 2027 enligt CRA ställer höga krav på beredskap. Policyn bör tydliggöra hur mottagare

ska hantera SBOM, integreras och hur krav ska utformas på leverantörer. En risk är att SBOM kommer att skapa stora administrativa bördor utan att organisationen har verktyg att hantera och analysera informationen. Om inte myndigheter och branschorganisationer, i samverkan med aktörer, tar fram operativt stöd riskerar mindre organisationer att inte förstå sina skyldigheter, vilket kan leda till försenade rapporter eller att sårbarheter inte åtgärdas. Det gäller även på global nivå. CVE-programmet visar att ett globalt system för sårbarhetsidentifiering inte bör vila på finansiering från en enskild stat. När MITRE:s amerikanska kontrakt höll på att löpa ut våren 2025 var programmet nära att stängas ned, vilket en analys pekar ut som en följd av att CVE-systemet uppfattas som ett amerikanskt verktyg och att denna ”single-nation ownership” hindrar globalt samarbete. Rapporten efterlyser därför en gemensam, internationell finansieringsmekanism. Policydokumentet noterar att EU redan har lanserat en europeisk sårbarhetsdatabas (EUVD) och att Enisa har blivit en central aktör i CVE-systemet för att minska beroendet av externa aktörer. Mot bakgrund av dessa erfarenheter bör Sverige verka för att EU-nivån får långsiktig finansiering för sådana system och att man undviker att skapa flera parallella rapporteringskanaler. I stället bör den nationella portalen integreras med EUVD och CVE så att det finns tydliga, gemensamma kontaktpunkter och ett robust, internationellt finansierat system för hantering av sårbarheter.

Mätbara mål för uppföljning och utvärdering

Målbilden 2029 anger att “över 50 procent av tillverkare” ska ha CVD-policy och att “minst 90 procent” av de som deltar i Cybersäkerhetskollen ska ha definierade processer och “minst 80 procent” uppger också att de har inventerat sina installerade programvaror som även innefattar programvaruförteckningar (SBOM). Det framgår dock inte hur nuläget ser ut, hur framsteg ska mätas eller vem som ansvarar för uppföljningen. Policyn bör ange baslinjer, mätbara indikatorer och rapporteringsrutiner. Det är viktigt att veta om och hur man kommer att omfattas av dessa uppföljningar då deltagande i Cybersäkerhetskollen är en bör-rekommendation och inte ett skall-krav.

Det öppna internets offentliga kärna (7.2 d)

Nulägesbild

Internetstiftelsen vill tillägga följande.

Internet är centralt i Sverige eftersom det bär samhällsviktiga tjänster som måste fungera robust, vilket kräver både fysisk och mjuk infrastruktur. Det innebär särskilt att konnektivitet och DNS fungerar från roten och nedåt—inklusive en nationellt fungerande rotzon—och att .se-toppdomänen kontinuerligt stärker robustheten, vilket Internetstiftelsen ständigt arbetar aktivt med.

Design av protokoll och standarder

Det finns fler än 1 300 rotserverinstanser över hela världen, vilka förvaltas och utvecklas av tolv organisationer i fyra länder koordinerade av ICANN.

Även om de ursprungliga versionerna av många Internetprotokoll inte uppfyller dagens krav på säkerhet har arbetet med att förbättra detta kommit långt. Problemet idag är ofta inte att det saknas säkra alternativ, utan att säkra alternativ uppfattas som alltför komplicerade och kostsamma att införa.

Specifikt när det gäller DNS så pågår sedan många år ett aktivt arbete med att göra hela "ekosystemet" runt DNS så säkert som möjligt. Detta arbete sker ofta nere på protokollnivå och koordineras då internationellt genom det som kallas IETF. Personal från Internetstiftelsen deltar aktivt, dels via egna förslag, dels som remissinstanser för utvärdering av andras förslag och arbete.

Ett av de viktigaste arbeten med att göra DNS säkrare är just nu, enligt Internetstiftelsens bedömning, det pågående projektet DNS TAPIR, vilket har fått finansiering både från PTS och Internetstiftelsen (utöver deltagande från flera andra centrala parter som Netnod och SUNET).

Målet med DNS TAPIR är en allmänt tillgänglig tjänst för hotanalys baserad på integritetssäker analys av aktuell DNS-trafik. Genom att göra resultaten allmänt tillgängliga är ambitionen att verka för en förbättrad DNS-säkerhet för hela samhället.

Nulägesanalys

Som en del av nulägesanalysen vill vi lyfta följande.

Ett väsentligt steg i arbetet med att stärka den offentliga kärnan i det öppna internet är att inventera samhällsviktiga funktioner och deras externa beroenden, samt testa dessa; det är vår bedömning att i dag saknas en samlad nulägesbild. Med en heltäckande nulägesbild kan därefter beroenden testas och vid behov stärkas.

Vi vill också lyfta att det inte är korrekt angivet att eftersom Sverige har en rotserver för DNS och därmed inte har något externt beroende för tillgång till listor över auktoritativa namnservrar, medför det goda förutsättningar för organisationer att införa DNSSEC. Rotserver för DNS och DNSSEC är två olika saker.

Utveckling och integrering av ny cybersäkerhetsteknologi (7.2 e)

Policyn trycker på användning av avancerad cybersäkerhetsteknik och standardiserade arbetssätt. För att uppfylla policyn krävs dock mer konkretisering, tydlig ansvarsfördelning, mätbara indikatorer, praktisk finansiering och harmoniserade definitioner. Policyn skulle behöva komplettera standarddefinitioner med nationella anpassningar och konkreta exempel, så att olika aktörer tolkar kraven på samma sätt.

Ett arbete som borde gå hand i hand med arbetet som MCF ansvarar för när det kommer till Termbanken.

För att svenska organisationer ska kunna ta till sig avancerad säkerhetsteknik, innebär detta nya arbetssätt och tid att förbereda sig för implementering av nya tekniska krav (AI, ML, Zero Trust, kvantsäker kryptografi och avancerad logganalys). Det behöver ställas krav på myndigheter att delta och bidra till standardiseringsarbete och säkerställa att resurser och stöd finns tillgängliga för att implementera avancerad säkerhetsteknik på ett effektivt och kostnadseffektivt sätt med standarder som grund.

Samordning med de andra policyområden är nödvändiga, detta då styrning av avancerad teknik (AI, ML, Zero Trust, kvantsäker kryptografi och avancerad logganalys) har en stark koppling till leverantörskedjor, upphandling och sårbarhetshantering. Här behöver myndigheter klargöra hur standarder, lagstiftning och arkitekturfrågor sammanflätas för att underlätta för små och medelstora företag att inte gå emot framtida rekommendationer. Därför är det bra att NCSC ser nyttan med att samverka med SIS TK318 för att tillsammans uppnå en synergi som gynnar alla som ska arbeta med det standardiserade arbetet.

Främja utbildning, forskning och ökad medvetenhet om cybersäkerhet (7.2 f)

Internetstiftelsen vill komplettera med följande avseende vårt arbete för ökad cybersäkerhetsmedvetenhet och cyberhygien i samhället.

Genom sina årliga rapporter Svenskarna och internet, med tillhörande delrapporter, bidrar Internetstiftelsen med insikter om vilka möjligheter och utmaningar svenskar möter i sin digitala vardag, vilka strategier de använder för att skydda sig och vara säkra samt vilka kompetensgap som behöver fyllas för att höja den breda allmänhetens digitala kompetens och säkerhet.

Internetstiftelsen tillhandahåller utbildningsinsatser, verktyg och kunskapsstöd som bidrar till kunniga och medvetna internetanvändare och stärker digital trygghet, motståndskraft och säkerhet. Under Internetkunskap.se samlas kostnadsfria guider, korta kurser och verktyg som hjälper människor att upptäcka risker, fatta bättre beslut online och skydda sig mot exempelvis bedrägerier och desinformation. Insatserna riktar sig brett till allmänheten, från barn i skolan till vuxna och seniorer, och kompletteras av Digitala lektioner, en kostnadsfri lektionsbank kopplad till skolans styrdokument.

Stärkt informationsdelning på cybersäkerhetsområdet (7.2 h)

Internetstiftelsen delar bedömningen att informationsdelning och samarbete mellan organisationer är avgörande för samhällets och verksamheters förmåga att förebygga, upptäcka och hantera cyberhot och incidenter. Dock behöver det lyftas att detta delvis bygger på frivillig informationsdelning, något som kan vara problematiskt i vissa fall, då

organisationer kanske inte alltid våga dela information då man inte vet var informationen hamnar.

I övrigt anser Internetstiftelsen att policyns innehåll är relevant och tydligt beskrivet.

Ökad cyberresiliens och cyberhygien hos små och medelstora företag (7.2 i)

Internetstiftelsen instämmer i vikten av att stärka cyberresiliens och cyberhygien hos små och medelstora företag (SMF). SMF är ofta både underleverantörer i samhällsviktiga leveranskedjor och beroende av komplexa digitala tjänster. Deras cybersäkerhetsförmåga påverkar därför samhällets samlade motståndskraft.

Internetstiftelsen vill dock särskilt lyfta följande. Resurs- och kompetensbrist är den största utmaningen. Krav och rekommendationer behöver därför vara proportionerliga och riskbaserade.

Internetstiftelsen välkomnar även ambitioner om regelförenkling, men vill betona att detta inte kommer avhjälpa regelbördan för alla mindre aktörer. Cybersäkerhetslagen/NIS2 gäller för vissa väsentliga verksamhetsutövare inom den digitala sektorn oavsett storlek. Dessa aktörer kommer fortsatt behöva konkret implementeringsstöd.

För Internetstiftelsen

Carl Piva