Myndigheten
för civilt försvar

Bilaga

Policyer för ett starkare cybersäkerhetsarbete

I enlighet med NIS 2-direktivets artikel 7.2 a)–f) och h)–j)

Policyer för ett starkare cybersäkerhetsarbete

Datum 2026-02-17
Ärendenummer 2025-03955

Myndigheten för civilt försvar
651 81 Karlstad

Innehåll

Bakgrund

NIS 2-direktivet syftar till att uppå en hög gemensam cybersäkerhetsnivå inom EU. NIS 2-direktivet infördes i svensk lagstiftning genom den nya Cybersäkerhetslagen som trädde i kraft den 15 januari 2026.

Enligt NIS 2-direktivets art. 7 ska varje medlemsstat ”anta en nationell strategi för cybersäkerhet som tillhandahåller strategiska mål, de resurser som krävs för att uppnå dessa mål och relevanta politiska och reglerande åtgärder, i syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå”.

Regeringen beslutade den 27 februari 2025 om att ge Försvarets radioanstalt (FRA) och Myndigheten för samhällsskydd och beredskap (numera Myndigheten för civilt försvar) i uppdrag att inom ramen för Nationellt cybersäkerhetscenter ta fram riktlinjer för art. 7.2 a-f och h-j. Art. 7 innehåller krav på att inom ramen för den nationella cybersäkerhetsstrategin inrikta arbetet inom tio områden. Mer specifikt framgår av art. 7.2 att medlemsstaterna som en del av den nationella cybersäkerhetsstrategin särskilt ska anta tio riktlinjer (översatt från engelskans policy). Policyerna är medlemsstatens viljeinriktning för vilken utveckling som ska ske inom de olika policyområdena och omfattas av sådana krav på strategin som beskrivs i art. 7.1. Myndigheten för civilt försvar och FRA/Nationellt cybersäkerhetscenter har, för att betona denna omständighet, valt att huvudsakligen benämna det som ska utvecklas som policyer.

Policyerna ska enligt regeringens uppdrag omfatta vägledande rekommendationer och utgöra ett stöd för verksamhetsutövare att prioritera rätt åtgärder för att på ett kostnadseffektivt sätt stärka sitt cybersäkerhetsarbete.

Uppdraget till Myndigheten för civilt försvar och FRA/Nationellt cybersäkerhetscenter omfattar att utveckla policy inom nio av de tio områdena:

- Stärkt säkerhet i digitala leveranskedjor 7.2a
- Cybersäker upphandling 7.2b
- Hantering av sårbarheter och sårbarhetsinformation 7.2c
- Det öppna internets offentliga kärna 7.2d
- Utveckling och integrering av ny cybersäkerhetsteknologi 7.2e
- Främja utbildning, forskning och ökad medvetenhet om cybersäkerhet 7.2f
- Stärkt informationsdelning på cybersäkerhetsområdet 7.2h
- Ökad cyberresiliens och cyberhygien hos små och medelstora företag 7.2i
- Främja ett aktivt cyberskydd 7.2j

Vetenskapsrådet har fått i uppdrag av regeringen att ta fram riktlinjer för art. 7.2g.

Målgrupper som har konsulterats

I framtagandet av detta arbetsdokument har externa synpunkter samlats in och hanterats. Utskick har gjorts till myndigheter och berörda parter specifikt. Utöver detta har synpunkter mottagits i samband med den externa konsultationen som initierades under Cybersäkerhetskonferensen och som var öppen för allmänheten.

Stärkt säkerhet i digitala leveranskedjor

Enligt NIS 2-direktivets artikel 7.2 a) Riktlinjer för cybersäkerhet i leveranskedjan för IKT-produkter och IKT-tjänster som används av entiteter när de tillhandahåller sina tjänster.

Definitioner och begrepp

Digital leveranskedja: Det nät av leverantörer, tjänster, system och underleverantörer som tillsammans möjliggör en digital tjänst eller produkt.

Digital suveränitet: En nations förmåga att kontrollera sina digitala beroenden, skydda sin information och minimera risken att påverkas av främmande staters jurisdiktion eller inflytande.

Diversifiering: En strategi där organisationer sprider sina beroenden över flera leverantörer eller tekniska lösningar för att minska risken för störningar och samhällspåverkan.

Diversifieringsgrad: Ett mått på hur beroenden är fördelade mellan olika leverantörer.

Inlåsningseffekt: Förhållanden som gör det svårt, kostsamt eller riskfyllt att byta leverantör, exempelvis på grund av specialanpassade lösningar, teknikval eller kontraktuella villkor.

Leveranskedjeincident: En händelse hos en leverantör eller underleverantör som påverkar mottagarens digitala tjänster, system eller information, oavsett om orsaken är fel, misstag, angrepp eller avbrott.

Mjukvarudeklaration (SBOM): En förteckning över alla komponenter, moduler och kodbibliotek som ingår i en programvara, vilket gör det möjligt att bedöma risker och sårbarheter.

Monoberoende: Ett läge där en organisation saknar realistiska alternativ till en specifik leverantör eller digital tjänst, vilket innebär att avbrott eller incidenter får oproportionerligt stora konsekvenser.

Nätverkseffekt: Ett fenomen där en tjänst blir mer attraktiv ju fler som använder den, vilket kan leda till marknadskoncentration och i förlängningen monoberoenden.

Redundans: Flera oberoende alternativ för att utföra samma funktion, så att verksamheten kan fortsätta även om en leverantör eller tjänst fallerar.

Secure by Design / Inbyggd säkerhet: Ett utvecklingssätt där säkerhet integreras från början i digitala produkter och tjänster.

Säker mjukvaruutveckling (SDLC): En strukturerad utvecklingsprocess där säkerhetskrav, tester och kontroller ingår i varje fas av mjukvarans livscykel.

Introduktion

Utgångspunkten i denna policy är att digitala leveranskedjor i Sverige präglas av hög tjänstekoncentration, återanvänd kod, komplexa beroenden och begränsad insyn hos leverantörer. Detta innebär att incidenter hos en enskild leverantör ofta får bred och ibland icke-linjär samhällspåverkan. Policyn utgår därför från behovet av att stärka verksamheters förmåga att identifiera, analysera och minska beroenden i sina digitala leveranskedjor, särskilt gällande monoberoenden och inlåsningseffekter.

För att förstå området behöver läsaren känna till företeelser såsom monoberoenden, viskleksproblematik, jurisdiktions- och suveränitetsrisker, återanvänd programvarukod och SBOM, samt hur nätverkseffekter bidrar till att leverantörsstörningar kan få omfattande konsekvenser.

Policyn relaterar till övriga policyområden, men avgränsas till vad som krävs för att minska risker och samhällspåverkan i digitala leveranskedjor.

Avgränsning

Denna policy (7.2a) fokuserar på säkerhet i digitala leveranskedjor: identifiering och hantering av beroenden, monoberoenden, inlåsningseffekter, jurisdiktionsrisker, uppdateringskedjor samt konsekvenser när sådant som inte ska levereras ändå levereras respektive när sådant som ska levereras inte levereras. Policyn behandlar vad som behöver göras för att minska samhällspåverkan kopplat till digitala leverantörsberoenden.

Nulägesbild

It-tjänstekoncentrationen i Sverige är hög. Det finns sammantaget ganska få leverantörer och många organisationer använder sig av samma leverantörer för samma slags tjänster. Många organisationer ingår därmed i samma digitala leveranskedjor, vilket i vissa fall leder till att monoberoenden etableras som en följd av nätverkseffekter. Ofta uppstår också inlåsningseffekter, dvs. omständigheter som gör det praktiskt mycket svårt att byta leverantör. När allt fler väljer en och samma tjänsteleverantör ges den tjänsteleverantören ekonomiska förutsättningar att stärka sitt erbjudande, vilket i sin tur gör att fler organisationer blir kunder till tjänsteleverantören, och ju mer utvecklad tjänsten som erbjuds är, desto svårare blir det att hitta en annan tjänst att byta till om en organisation skulle önska det.

Ett högt antal kunder hos en och samma tjänsteleverantör innebär också att den tjänsteleverantören får ekonomiska förutsättningar att finansiera en högre grad av säkerhet i sina system och tjänster. Samtidigt innebär det höga antalet kunder hos en och samma leverantör att en incident hos densamme kan medföra bred samhällspåverkan. Samma omständigheter som gör att det finns goda möjligheter till hög robusthet har alltså samtidigt inneburit att incidenter, när de trots robustheten ändå inträffar, kan få större samhällspåverkan.

Detta återspeglas tydligt i den nationella statistiken för it-incidentrapporteringen. I rapporten Hoten mot de digitala leveranskedjorna[1] rapporterade Myndigheten för samhällsskydd och beredskap år 2021 att:

> Sedan början på 2020 och fram till slutet på juni 2021 har två tredjedelar av alla inrapporterade incidenter hos leverantörer av samhällsviktiga eller digitala tjänster haft sitt ursprung i en leveranskedja.

Myndigheten för samhällsskydd och beredskaps årsrapporter för it-incidentrapporteringen[2] har därefter årligen visat att en hög andel av de rapporterade incidenterna har inträffat hos en leverantör av en tjänst som den rapporterande verksamhetsutövaren använder sig av.

De vanligaste kända orsakerna till leveranskedjeincidenter i Sverige har, i likhet med andra kategorier av incidenter, varit misstag och systemfel. Naturhändelser som bakomliggande orsak är mer sällsynt i rapporteringen, men har globalt resulterat i bl.a. avbrott i tillverkning av fysiska komponenter (exempelvis i samband med en snöstorm och extrem kyla i Texas under februari 2021[3]) som behövs för upprättande, återställning respektive utveckling av informationssystem. Samtidigt har de leveranskedjeincidenter som har haft de mest allvarliga konsekvenserna i Sverige (Kaseya-incidenten[4], Tietoevry-incidenten[5] och Miljödata-incidenten[6, 7]) de senaste åren alla orsakats av angrepp. Då de rapporterande organisationerna ofta har haft begränsad insyn i vad som har hänt hos deras leverantörer (och i de flesta *ingen* direkt insyn i vad som har hänt hos deras leverantörers leverantörer) så har det årligen också varit en hög andel

[1] https://www.Myndigheten för civilt försvar.se/sv/publikationer/hoten-mot-de-digitala-leveranskedjorna--50-rekommendationer-for-att-starka-samhallssakerheten/
[2] https://www.Myndigheten för civilt försvar.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/hantera-och-rapportera-it-incidenter-och-cyberangrepp/arsrapporter-om-it-incidenter-och-cyberangrepp/
[3] https://www.bbc.com/news/technology-56114503
[4] https://www.cisa.gov/news-events/news/kaseya-ransomware-attack-guidance-affected-msps-and-their-customers
[5] https://www.svt.se/nyheter/inrikes/120-myndigheter-drabbade-av-it-attack-tiotusentals-anstallda
[6] https://www.svt.se/nyheter/inrikes/miljodata-aterstallningen-ar-snart-klar
[7] https://www.svt.se/nyheter/inrikes/experten-en-miljon-svenskars-personuppgifter-publicerade-pa-darknet

rapporter som beskriver leveranskedjeincidenter och där det anges att orsaken till incidenten är okänd.

Ett relaterat fenomen som bl.a. beror på den bristande insynen hos leverantörer är så kallad viskleksproblematik. Det betyder att information som upprättas och skickas vidare av en organisation långt ”uppströms” i kedjan, successivt tolkas och i tolkat format adderas till, reduceras från och vidarebefordras till organisationer nedströms. Det kan ofta ske på ett sätt som gör att den information som ursprungligen förmedlades inte är densamma som den information som når organisationer några steg längre ned i kedjan. Det leder till att organisationer får svårt att ta välgrundade beslut om hur de ska agera när incidenter sker, eller att de får en felaktig bild av vad som behöver göras och därför fattar olämpliga beslut.

Samhällskonsekvenser av incidenter i digitala leveranskedjor

Incidenter i digitala leveranskedjor får olika grad av samhällspåverkan i olika delar av landet beroende på huruvida boende och organisationer i lokalområdet har monoberoenden till någon eller några organisationer som drabbats av en sådan incident. Kaseya-incidenten drabbade organisationer inom bl.a. dagligvaruhandel (Coop) och apoteksverksamhet (Apoteket Hjärtat).[8] Konsekvenserna av incidenten varierade över landet. I områden där det finns flera apotekskedjor var det fortfarande möjligt att hämta ut medicin hos kedjor som nyttjade ett annat betalsystem än det som hade infekterats med ransomware. På vissa platser i Norrland, där det exempelvis endast fanns en Coop-butik, innebar incidenten att boende under ett par eller några dagar fick resa långa avstånd för att få tag i dagligvaror.

Incidenter hos mycket stora it-tjänsteleverantörer kan också *få icke-linjära konsekvenser* för mottagare av den drabbade tjänsten. I samband med Tietoevry-incidenten förlorade först vissa regioner åtkomst till information och tjänster som de hyrde från Tietoevry. Därefter upptäckte de också att deras leverantörer av vissa typer av varor och artiklar också nyttjade tjänster från Tietoevry, varför det ett tag såg ut som att det kunde bli problem med att få även sådana leveranser.[9]

Ökad medvetenhet om risker med digitala leveranskedjor

De påtagliga konsekvenser som vissa leveranskedjeincidenter har haft har de senaste åren lett till en ökad medvetenhet bland såväl allmänheten som hos organisationer om vikten av att stärka säkerheten i de digitala leveranskedjor de nyttjar. Det finns dock en viss variation. Hos små och medelstora företag har utvecklingen inte varit lika påtaglig. Samtidigt har nya incidenter fortsatt att

[8] https://www.svt.se/nyheter/inrikes/it-attacken-mot-coop-detta-har-hant
[9] https://lakartidningen.se/nyheter/hackerattacken-som-skakade-samhallet/

inträffa. Det är oklart om den ökade medvetenheten har lett till ett förstärkt cybersäkerhetsarbete hos leverantörer generellt. Den genomsnittliga deltagande organisationen i Cybersäkerhetskollen 2025 hade inte heller uppnått lägstanivån inom dem fem arbetsområden som täcktes. Inom områdena kravställning samt incidenthantering var det överlag bättre resultat, men inom de resterande områdena såsom uppföljning, säkra leveranser samt riskhantering är det tydligt att det finns många utmaningar innan medvetenheten och det aktiva cyberskyddet når dem nivåer som behövs för att minska sårbarheter och förhindra incidenter.

Initiativ som syftar till att stärka säkerheten i digitala leveranskedjor

Den ökade medvetenheten om risker kopplade till digitala leveranskedjor har resulterat i att nya tjänster för att hantera sådana risker har utvecklats på olika nivåer och inom såväl staten som det privata näringslivet.

På EU-nivå är arbetet med att ta fram en verktygslåda för att stärka säkerheten i digitala leveranskedjor nu i sin slutfas.[10] Ett antal olika områden är också föremål för analys i enlighet med NIS 2-direktivets artikel 22. Sverige, genom Myndigheten för civilt försvar, har som ett av ordförandeländerna i arbetsgruppen som driver arbetet haft en ledande roll.

I Sverige har regeringen gett Myndigheten för civilt försvar i uppdrag att genomföra en kartläggning av digitala leveranskedjor och ta fram en modell för uppföljning av digitala leveranskedjor.[11] Uppdraget har resulterat i att Myndigheten för civilt försvars verktyg Cybersäkerhetskollen numera inkluderar verktyget Leveranskedjekollen. Leveranskedjekollen tillhandahölls för första gången till svenska organisationer under 2025. Myndigheten för civilt försvar har också etablerat möjligheter för svenska organisationer att vända sig till myndighetens tjänst Cybersäkerhetsrådgivningen för att ställa frågor om säkerhet i digitala leveranskedjor. Ett arbete har också inletts på myndigheten för att utvidga tjänsten Metodstödet, så att organisationer ska ha ett mer fullödigt material om säkerhet i digitala leveranskedjor att nyttja för självstudier. Även andra myndigheter har tagit fram stöd. Exempelvis har Upphandlingsmyndigheten tagit fram stöd för utarbetandet av krav på bl.a. säkerhet vid upphandling[12] och Tillväxtverket kartlagt små och medelstora företags förutsättningar att arbeta med bland annat säkerhet i digitala leveranskedjor.[13]

---

[10] https://www.mlex.com/mlex/technology/articles/2392767/eu-toolbox-for-managing-blocking-high-risk-digital-suppliers-almost-ready
[11] Fö2025/00390
[12] https://www.upphandlingsmyndigheten.se/om-hallbar-upphandling/socialt-hallbar-upphandling/arbetsrattsliga-villkor/ansvarsfulla-leveranskedjor/
[13] Se exempelvis https://techtidningen.se/molnet-unik-genomgang-sa-stor-ar-microsoft-dominansen-ute-bland-kommunerna/. För mer information om situationen i EU i stort, se https://tillvaxtverket.se/tillvaxtverket/publikationer/publikationer2021/sakerdigitaliseringismaochmedelstoraforetag.1427.html

Parallellt med utvecklingen av de ovan nämnda stödtjänsterna utvecklar Myndigheten för civilt försvar, i nära samarbete med de myndigheter som har föreslagits bli tillsynsmyndigheter utifrån Cybersäkerhetslagen och Cybersäkerhetsförordningen, nya föreskrifter som bl.a. konkretiserar kraven i NIS 2-direktivets artikel 21 p. 2d om stärkt säkerhet i digitala leveranskedjor.

Samtidigt som myndigheterna har stärkt sitt arbete på området så har också det privata näringslivet utvecklat nya tjänster. Det finns idag ett brett utbud av såväl tekniska tjänster som olika utbildningar, rådgivningstjänster, stöd i utarbetandet av krav och andra delar.

För att ytterligare stärka det privata näringslivets tjänsteutbud avseende hantering av säkerhet i digitala leveranskedjor genomförde Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet, NCC-SE (en del av Myndigheten för civilt försvar) också under 2025 en utlysning om finansiellt stöd till tredje part. Utlysningen utmynnade i att myndigheten beslutade om att stödja 25 nya projekt med ett samlat värde motsvarande totalt 34 miljoner kronor.[14]

Digital suveränitet

Svenska organisationers beroende av digitala produkter som levereras av organisationer med säte respektive majoritetsägare utanför EU är mycket stort.[15]

Digitala leveranskedjor utnyttjas för problematisk eller antagonistisk aktivitet på andra sätt än genom cyberangrepp. Monoberoenden till digitala leveranskedjor som står under andra jurisdiktioners kontroll har utnyttjats, och fortsätter att utnyttjas, av andra stater utifrån säkerhets- och/eller geopolitiska intressen. Hot om att stänga av leveranser som samhällen har monoberoenden till används för att sätta press i syfte att få stater, eller organisationer i stater, att agera respektive avstå från att agera på vissa sätt. I vissa fall har dessa hot agerats på, exempelvis för att hämma eller sabotera aktivitet som anses gå emot de egna intressena.

Stater som har inflytande över leverantörer använder sådant inflytande för att driva egna intressen även när organisationer har egna, fristående och lokalt installerade digitala produkter, exempelvis genom att förhindra försörjning av komponenter, eller av säkerhetsuppdateringar som behövs för att hantera upptäckta sårbarheter. Det omvända förekommer också, när stater utnyttjar sin kontroll för att antingen (i skymundan och utan leverantörens vetskap) introducera

[14] https://ncc-se.Myndigheten för civilt försvar.se/sv/nyheter/Myndigheten för civilt försvar-beviljar-stod-till-25-nya-cybersakerhetsprojekt-for-att-starka-sveriges-digitala-leveranskedjor/

[15] https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778576/ECTI_STU%282025%29778576_EN.pdf

cyberhot i leverantörens digitala produkter, eller för att tvinga leverantören att själv introducera cyberhot i sina digitala produkter.

Juridisk kontroll används därutöver för att tilltvinga sig tillgång till information som flödar fram och tillbaka genom digitala leveranskedjor inom allt ifrån telekominfrastruktur till uppkopplade fordon.

Den legala utvecklingen inom EU

För att hantera de komplexa säkerhetsutmaningarna kopplat till säkerhet i digitala leveranskedjor, inklusive den växande problematiken med statlig inblandning och statliga ingripanden i sådana leveranskedjor, har det införts, och fortsätter att införas, ny lagstiftning för att öka säkerheten. Den legala utvecklingen kan delas in i tre kategorier, reglering av säkerhet i digitala leveranskedjor där:

1. både leverantör och mottagare, respektive deras ägare, finns inom EU,
2. leverantören eller dess ägare finns utanför EU och mottagaren och dess ägare finns inom EU,
3. leverantören och dess ägare finns inom EU och mottagaren eller dess ägare finns utanför EU.

I den första kategorin ingår krav på organisationer, både leverantörer och mottagare, att stärka sin insyn i, kontroll över och säkerhet i digitala leveranskedjor (exempelvis med stöd av NIS 2-direktivets artikel 21 p. 3), särskilda insatser för att öka säkerheten i vissa särskilt viktiga digitala leveranskedjor (i EU med stöd av NIS 2-direktivets artikel 22) och krav på att utveckla och tillhandahålla produkter som har tagits fram enligt *security by design*-principer (med stöd av Cyberresiliensförordningen). Det ingår också i regleringarna att tillsyn ska utövas av ansvariga myndigheter för att säkerställa att regelverket efterlevs, och tillsynsmyndigheterna har relativt kraftfulla verktyg för att sanktionera bristande regelefterlevnad.

I den andra kategorin har det införts legala ramverk för att kunna besluta om såväl handelshinder och som begränsningar av utom-jurisdiktionellt ägande i vissa industrier och teknologier (såsom Europaparlamentets och rådets förordning (EU) 2019/452 av den 19 mars 2019 om upprättande av en ram för granskning av utländska direktinvesteringar i unionen). EU-kommissionen har också tagit initiativ till att uppdatera EU:s Cybersäkerhetsförordning, och har i anslutning till det öppnat för att införa ett legalt ramverk för att hantera icke-tekniska aspekter på säkerhet i digitala leveranskedjor. Förslaget innebär en långtgående rätt för EU-kommissionen att både, på olika sätt, stoppa eller begränsa s.k. högriskleverantörers verksamhet på den inre marknaden, men också att tvinga

verksamhetsutövare som omfattas av NIS 2-direktivet att ta bort komponenter och system ur sina it-miljöer som kommer ifrån en högriskleverantör.[16]

Befintligt lagrum nyttjas också för att begränsa utom-juridiskt inflytande över upphandlade tjänster, såsom i fallet där Arbetsförmedlingen uteslöt anbudsgivare med ägaranknytning till länder som Säkerhetspolisen har pekat ut som hot mot Sverige.[17]

I den tredje kategorin kan exempelvis inräknas EU-förordningen 2021/821 om upprättande av en unionsordning för kontroll av export, förmedling, transitering och överföring av, samt tekniskt bistånd för produkter med dubbla användningsområden.[18]

En konsekvens av den ökade styrningen, och den tillkommande komplexiteten som kommer genom nya lagkrav, är att det blir dyrare och svårare att göra affärer inom berörda sektorer. Många organisationer upplever att den stora mängden krav som följer av ett stort antal olika lagar som organisationer måste följa samtidigt innebär att stora resurser måste läggas på att identifiera den samlade kravbilden och regelefterlevnad.[19]

När sådant som inte ska levereras ändå levereras

Det finns två typer av risk i digitala leveranskedjor. Den första sortens risk handlar om att mottagande organisationer *får* något skickat till sig som de *inte ska ha* och behandlas i detta avsnitt. Den andra risken behandlas i nästföljande avsnitt.

En drivande faktor i nyttjandet av digitala leveranskedjor är att mottagande organisationer i allmänhet försöker uppnå maximal effektivitet i hanteringen av det som levereras genom att endast i begränsad omfattning granska och testa det som skickas till dem inom ramen för den digitala leveranskedjan. Ofta finns det en förberedd kanal in i organisationen som ska minimera tiden mellan mottagande och installation och tillämpning. Detta gäller i synnerhet mjukvaruuppdateringar. Mottagande organisationer upprättar en sådan kanal när de har förtroende för avsändaren och när de har stor nytta av att uppdateringen installeras snabbt och i alla relevanta delar av organisationens it-miljö. Om det som har levererats då är skadlig kod, eller skadlig kod ingår som en komponent i en uppdatering, kan stor skada uppkomma innan organisationen inser vad som har hänt eller kan göra något för att stoppa den skadliga utvecklingen. Även om det är ovanligt så förekommer det att motsvarande händer med fysiska komponenter. Det blev inte minst blev tydligt i samband med att personsökare som hade levererats till den

[16] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act
[17] https://www.dagensjuridik.se/nyheter/domstol-kinesiskt-agande-kan-utesluta-bolag-fran-upphandling/
[18] https://isp.se/produkter-med-dubbla-anvandningsomraden/introduktion-till-pda/
[19] https://www.svensktnaringsliv.se/english/simplifying-the-eus-digital-regulatory-framework_1233384.html

libanesiska organisationen Hizbollah i september 2024 exploderade efter att en i hemlighet inbyggd spränganordning i personsökarna nåddes av en given signal – något som ledde till flera dödsfall och många skadade.[20]

Ett specialfall av den här problematiken rör säkerhetsuppdateringar. Generellt är rådet som ges till organisationer att de ska installera säkerhetsuppdateringar så fort och så brett som möjligt. Genom att göra det så förebyggs angripares möjligheter att genomföra angrepp med hjälp av sårbarheten som säkerhetsuppdateringen åtgärdat. Det är vanligt att säkerhetsuppdateringar släpps precis innan, och ibland samtidigt, som angrepp som bygger på sårbarheten genomförs. Men om säkerhetsuppdateringen i sig innehåller skadlig kod så kan ambitionen att snabbt säkerställa att organisationen har ändamålsenligt it-skydd innebära att desto mer skada orsakas istället.

En ytterligare problematik kopplat till uppdateringar består i att tjänster som upprätthåller säkerheten i it-miljöer oftast har (för att de behöver ha) djupgående tillgång och rättigheter till konfigurationer och kärnsystem för att dels kunna upptäcka, och dels (genom att ha ändringsrättigheter) kunna bekämpa antagonistisk aktivitet. Skadlig kod som ingår i uppdateringar till sådana tjänster får därför direkt möjlighet att orsaka skada på djupare nivåer eller i mer skyddsvärda miljöer än skadlig kod som kommer in i miljön på andra sätt. Ett globalt uppmärksammat exempel på det var Crowdstrike-incidenten 2024.[21]

Utveckling av programvara är en komplex process som ofta innebär att kod som redan har tagits fram i andra sammanhang, och som utför en viss sorts funktion, introduceras i en större uppsättning kod för att skapa en komplex produkt med många olika funktioner. Koden som återanvänds hämtas ifrån kodbibliotek och koden som finns i sådana bibliotek underhålls och utvecklas av organisationer och individer som organisationen som ska använda koden kanske aldrig har haft kontakt med, eller vet vilka de är. Den här omständigheten resulterar i att organisationer inte alltid vet vad koden de har i sina egna produkter kommer att göra givet olika typer av inputs, eller givet vilken miljö koden introduceras i. För att hantera den här utmaningen har olika initiativ om programvaruförteckningar (*Software Bill of Materials*, SBOM[22]) växt fram. Att underhålla sådana förteckningar är dock resurskrävande och initiativen har fått begränsat genomslag.

Det höga antalet kunder, den snabba och förtroendebaserade process som organisationer följer när de installerar i synnerhet mjukvara som de mottar och den djupa tillgången till system och tjänster som i synnerhet it-säkerhetstjänster måste ha gör att leverantörer av it-tjänster i allmänhet, och leverantörer av it-säkerhetstjänster i synnerhet, utgör lockande mål för hotaktörer som önskar sprida

[20] https://en.wikipedia.org/wiki/2024_Lebanon_electronic_device_attacks
[21] https://en.wikipedia.org/wiki/2024_CrowdStrike-related_IT_outages
[22] https://about.gitlab.com/blog/the-ultimate-guide-to-sboms/

skadlig kod till många, eller till mål som i övrigt är väl skyddade. Intresset för leverantörer tar sig båda i uttryck genom cyberangrepp, men också genom att stater utövar juridiskt och annat inflytande över sådana leverantörer på sådana sätt som har beskrivits ovan.

När sådant som ska levereras inte levereras

Det finns två typer av risk i digitala leveranskedjor. Den andra sortens risk handlar om att mottagande organisationer *inte får* något skickat till sig som de *ska ha* och behandlas i detta avsnitt. Den andra risken behandlas i föregående avsnitt.

Den vanligaste formen av digital leveranskedjeincident är avbrott i en sådan tjänst som en tjänsteleverantör tillhandahåller till andra.

Det är vanligt att organisationer saknar redundans i sina tjänster, varför uteblivna leveranser av digitala produkter från en leverantör innebär att produktion eller verksamhet avstannar, eller åtminstone tappar påtagligt i effektivitet och takt.

Det förekommer också att digitala produkter levereras, men saknar sådana komponenter (i form av funktionalitet eller skydd) som den mottagande organisationen förväntar sig, eller har uppfattat, ska ingå i den digitala produkten. När sådan hård- eller mjukvara installeras och används uppstår problem när förväntade funktioner eller effekter visar sig saknas eller inte uppstå. På motsvarande sätt exponerar organisationer som installerar nya digitala produkter som de tror har ett adekvat skydd, men som i själva verket inte har det, sig för angrepp eller misstag som de inte förväntar sig ska kunna vara skadliga för dem.

Ett vanligt fenomen är att en tjänsteleverantör, för att kunna leverera en viss tjänst, samtidigt också måste vara mottagare av stora mängder information ifrån de som tjänsten ska levereras till. Exempelvis kan lagrings- respektive bearbetningstjänster endast göra nytta om de ges information att lagra eller bearbeta. När många organisationer lagrar eller bearbetar sin information hos samma leverantör kan det därför, om det uppstår en incident hos leverantören, bli så att de organisationernas information raderas eller otillbörligen tillgängliggörs. Detta blev i Sverige påtagligt i samband med Miljödata-incidenten 2025, under vilken bl.a. HR-tjänsterna Miljödata tillhandahåller angreps, varpå informationen som hade lagrats däri sedermera publicerades på Darknet.

Analys av nuläget

Det är positivt att medvetenheten om riskerna kopplat till digitala leveranskedjor har ökat, och att det har resulterat i att såväl staten som det privata näringslivet har utvecklat nya tjänster för att underlätta arbetet med att stärka säkerheten. Det är också positivt att ny lagstiftning, såsom NIS 2-direktivet, DORA-förordningen och Cyberresiliensförordningen, har tillkommit och ställer krav på ökad säkerhet i digitala leveranskedjor. Därtill är det positivt att individer och organisationer i

medelstora och större orter i landet, där det finns fler än en leverantör av viktiga samhällsfunktioner som var för sig har olika digitala leveranskedjor, (åtminstone i viss utsträckning) kan kompensera för bortfallet av en viss leverantörs samhällsviktiga funktion (såsom telenät, dagligvaruhandel, etc.) genom att vända sig till en annan.

Samtidigt finns ett antal utmaningar inom området:

1. Incidenter i digitala leveranskedjor fortsätter att inträffa i oförminskad årlig frekvens. Incidenter som inträffar hos leverantörer av digitala produkter får ofta inverkan på många andra organisationer som drabbas i förlängningen. Incidenterna orsakas av såväl misstag och systemfel som av angrepp.
2. Förekomsten av monoberoenden och inlåsningseffekter. När incidenter inträffar hos leverantörer som det finns ett monoberoende till så uppstår ofta en påtagligt värre samhällspåverkan än när samma slags incidenter inträffar hos andra organisationer. Monoberoenden uppstår som en följd av nätverkseffekter.
3. Stater utnyttjar att monoberoenden har uppstått i förhållande till leverantörer som de kan utöva inflytande över, eller ingripa hos, som ett sätt att hota eller påverka andra stater och i syfte att uppnå säkerhets- eller geopolitiska mål. Sådant inflytande orsakas av att vissa tjänsteleverantörer har ett tekniskt och tjänstemässigt försprång gentemot lokala alternativ, och det försprånget innebär att nätverkseffekter uppstår, varpå monoberoenden resulterar.
4. Incidenter (i form av att sådant som ska levereras inte levereras) som inträffar hos tjänsteleverantörer som har många kunder resulterar ibland i icke-linjära konsekvenser för mottagare av den eller de drabbade tjänsterna. När mottagare av den drabbade tjänsten också nyttjar tjänster ifrån andra organisationer som också nyttjar den drabbade tjänsten kan de drabbas dubbelt. Först genom att de förlorar åtkomst till sin information och tjänsterna de använder, och därefter genom att andra leveranser som de också ska ha uteblir eftersom leverantören av de leveranserna också har förlorat åtkomst till tjänster de är beroende av för att kunna genomföra sin verksamhet. Sådana icke-linjära konsekvenser orsakas också av nätverkseffekter.
5. Incidenter (i form av att sådant som inte ska levereras ändå levereras) sker och får allvarligare konsekvenser genom att skadliga digitala produkter levereras inom ramen för en förtroendebaserad process där endast begränsad granskning och testning sker, och målet är snabb och bred implementering. Sådana allvarligare konsekvenser möjliggörs och orsakas av att det ofta finns goda skäl för organisationer att arbeta på ett sådant sätt.

6. Leverantörer av digitala produkter, framförallt it-tjänsteleverantörer, och i synnerhet it-säkerhetstjänsteleverantörer, utgör särskilt intressanta mål för hotaktörer. När cyberangreppsförsök mot sådana organisationer lyckas så får det typiskt sett följdkonsekvenser för många andra organisationer. Hotaktörers incitament att angripa sådana organisationer orsakas av att de har många kunder, att de har förtroendebaserade processer (processer där granskning och testning endast genomförs i begränsad utsträckning) för att överföra och installera sina digitala produkter hos sina kunder och för att deras produkter (i synnerhet vad gäller it-säkerhetstjänsteleverantörer) ofta måste ha djupgående tillgång och rättigheter i mottagarnas it-miljöer.
7. Många organisationer har bristande insyn hos sina leverantörer, och får begränsat med information – ibland med en tidsfördröjning – vilket gör att möjligheten att mildra incidenters konsekvenser blir begränsad. Den bristande insynen är ett resultat av otillräcklig kravställning när tillhandahållandet av tjänsten har avtalats.
8. Många organisationer har också begränsad insyn i vad koden de nyttjar ifrån andra källor har för funktion, eller hur dess funktion förändras när den genomgår uppdateringar. Det leder till att skadlig kod kan inkluderas i kod som i övrigt fyller en viktig funktion i olika sorters programvara, utan att den som använder koden i sin digitala produkt vet om det. Problematiken orsakas av att det är ekonomiskt mycket fördelaktigt att kunna återanvända redan producerad kod som man vet att man själv, eller andra, tidigare har sett göra sådant som man behöver ha kod för att göra. Det har därför växt fram ett förtroendebaserat system för vidareutnyttjande av kod som kan utnyttjas av hotaktörer för att introducera medvetet utvecklad skadlig kod, men som också kan resultera i att oupptäckta buggar introduceras i stora mängder kod hos olika organisationer.
9. Viskleksproblematik uppkommer när incidenter i digitala leveranskedjor får konsekvenser i flera led och information inte delas transparent mellan alla led. Detta hämmar förmågan att begränsa incidenters konsekvenser hos organisationer i det andra ledet, och organisationer i ytterligare led efter dem. Viskleksproblematik blir resultatet när information om det inträffade inte delas publikt, och information om det inträffade delas typiskt sett enbart publikt om det finns tydliga lagkrav om det eller om det ligger i den drabbade organisationens eget intresse att informera om det inträffade.
10. Stora mängder (ofta skyddsvärd) information koncentreras hos vissa leverantörer. För att tjänsten som en leverantör tillhandahåller ska kunna fungera krävs ofta att mottagaren av tjänsten överför sin information. Det leder till att många organisationer sparar sin (ibland känsliga) information på ett och samma ställe. Det kan i sin tur leda till att många organisationer samtidigt får sin information raderad, eller exponerad, när en incident

inträffar hos leverantören. Problematiken orsakas inte av någon särskild faktor, utan är en del av själva tjänstemodellen.

Regleringen av området är inte samlad, utan kommer ifrån ett antal olika lagar. Det får till konsekvens att det blir svårt för organisationer att överblicka vad de förväntas göra. Det förekommer också att organisationer upplever att det är svårt att sammanställa en samlad kravbild, inte minst då det är olika ansvariga myndigheter (som huvudsakligen har kunskap och kompetens inom den del av området som de har ansvar för) som måste konsulteras för att (exempelvis) förtydliga hur lagtext ska förstås. Utmaningen är orsakad av en blandning av faktorer som har att göra med att området överlappar med många andra områden som var för sig har egen reglering och att lagstiftaren de senaste åren har sett behov av att ytterligare reglera området med anledning av bland annat hotbildsutvecklingen.

Målbild 2029

När verksamhetsutövare som levererar digitala produkter nämns nedan så avses alla verksamhetsutövare i Sverige som levererar digitala produkter och som omfattas av Cybersäkerhetslagen själva, respektive alla verksamhetsutövare i Sverige som levererar digitala produkter till minst 5 verksamhetsutövare som var för sig omfattas av Cybersäkerhetslagen.

Färre leveranskedjeincidenter

Vid slutet av år 2029 har mindre än 20 digitala leveranskedjeincidenter där 20 eller fler mottagare har drabbats inträffat under det senaste året. När leveranskedjeincidenter har inträffat så har verksamhetsutövare som levererar digitala produkter samarbetat och delat information med sina mottagare. Verksamhetsutövare som omfattas av Cybersäkerhetslagen har prioriterats i incidenthantering och återställning.

Utvecklad förmåga hos leverantörer av digitala produkter

Vid slutet av år 2029 bedrivs ett systematiskt cybersäkerhetsarbete av verksamhetsutövare i Sverige som levererar digitala produkter.

Vid slutet av år 2029 informerar verksamhetsutövare i Sverige som levererar digitala produkter sina mottagare fortlöpande om sitt systematiska cybersäkerhetsarbete, kommande ändringar och uppdateringar samt vid incidenter i ett tidigt skede och sedan fortlöpande med relevant och tillräckligt omfattande information.

Vid slutet av år 2029 har och tillämpar leverantörer av digitala produkter en etablerad standard som gör att mottagare av deras digitala produkter både för övergripande och detaljerad information om justeringar i, uppdateringar av, tillägg

till, respektive borttagande av komponenter i digitala produkter som de själva, och deras leverantörer, har gjort.

Utvecklad förmåga hos mottagare av digitala produkter

Vid slutet av år 2029 bedrivs ett systematiskt cybersäkerhetsarbete av verksamhetsutövare i Sverige som omfattas av Cybersäkerhetslagen och mottar digitala produkter.

Sådana verksamhetsutövare har avtal med sina leverantörer av digitala produkter som innebär att de får det som ska levereras, att de inte får det som inte ska levereras, att de utifrån sina behov tidigt och fortlöpande får relevant och tillräcklig information om inträffade incidenter så att de kan bedöma konsekvenser och planera incident- respektive kontinuitetshantering samt att de prioriteras framför andra kunder vid incidenthantering och återställning.

Sådana verksamhetsutövare har och följer rutiner för att ta emot, verifiera, och implementera digitala produkter. De har, övar och tillämpar rutiner för incidenthantering för att bättre kunna hantera när digitala produkter som inte ska levereras ändå levereras. Därutöver har, övar och tillämpar de rutiner för kontinuitetshantering för att mer effektivt kunna bedriva verksamhet när något som inte ska levereras ändå levereras respektive när något som ska levereras inte levereras.

Proaktiv hantering av leveranskedjeincidenter

Vid slutet av 2029 finns och används en förmåga att snabbt kartlägga, och kontinuitetsplanera utifrån, digitala leveranskedjeincidenters direkta, såväl som icke-linjära, konsekvenser när sådana incidenter uppstår. När en leverantör av digitala produkter drabbas av en incident som får negativ påverkan på mottagare av de digitala produkterna så kan de mottagarna snabbt bedöma de samlade konsekvenserna som det inträffade kommer att ha för dem, dels i form av direkta konsekvenser (såsom att tjänsten de hyr av leverantören inte längre levereras), dels i form av icke-linjära konsekvenser (såsom att leverantörer av andra tjänster eller produkter som de har också har drabbats av konsekvenserna av incidenten hos leverantören av den digitala produkten).

Brutna monoberoenden och inlåsningseffekter samt minskat inflytande för främmande makt över digitala leveranskedjor

Vid slutet av år 2029 finns en nationell plan för hur riskerna med monoberoenden och inlåsningseffekter ska hanteras och förebyggas, samt hur den digitala suveräniteten ska stärkas såväl nationellt som inom EU, inklusive nationella mål för vad som ska uppnås. Planen genomförs inom ramen för ett etablerat samarbete mellan centrala myndigheter med uppdrag inom utländska direktinvesteringar, samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor, och upphandlingar.

Åtgärder för att uppnå målbilden

När verksamhetsutövare som levererar digitala produkter nämns nedan så avses (om inget annat anges) alla verksamhetsutövare i Sverige som levererar digitala produkter och som omfattas av Cybersäkerhetslagen själva, respektive alla verksamhetsutövare i Sverige som levererar digitala produkter till minst fem verksamhetsutövare som var för sig omfattas av Cybersäkerhetslagen.

Åtgärder som kommer att vidtas av det nationella cybersäkerhetscentret och dess partners

1. Under 2026–2027 uppdatera och utveckla Metodstödet för systematiskt cybersäkerhetsarbete så att det finns stöd till verksamhetsutövare som är, eller ska bli, mottagare av digitala produkter att:

- ställa relevanta och tillräckliga krav vid upphandling och kontraktering,
- utvärdera och följa upp ställda krav,
- upprätta, underhålla, utveckla och tillämpa rutiner för att:
    - ta emot, verifiera, och implementera digitala produkter
    - hantera leveranskedjeincidenter,
    - kontinuitetshantera vid leveranskedjeincidenter,
- öva incidenthantering respektive kontinuitetshantering vid leveranskedjeincidenter,
- klara kraven på säkerhet i digitala leveranskedjor i Myndigheten för civilt försvars, från och med 1 juli 2026 FRA/Nationellt cybersäkerhetscenters, föreskrifter för verksamhetsutövare som omfattas av Cybersäkerhetslagen respektive myndigheter som omfattas Förordning (2022:524) om statliga myndigheters beredskap.

2. Under 2026–2027 uppdatera och utveckla Metodstödet för systematiskt cybersäkerhetsarbete så att det finns stöd till verksamhetsutövare som är, eller ska bli, leverantörer av digitala produkter att:

- strukturerat informera om genomförda, pågående respektive planerade ändringar och uppdateringar samt om inträffade och pågående respektive avslutade incidenter,
- ge mottagare övergripande respektive detaljerad information om justeringar i, uppdateringar av, tillägg till, respektive borttagande av komponenter.

3. Under 2026–2027 över behovet av att ytterligare utveckla Leveranskedjekollen (som är en del av tjänsten Cybersäkerhetskollen) för att möjliggöra uppföljning och planering av det systematiska cybersäkerhetsarbetet med digitala leveranskedjor för såväl mottagare som leverantörer av digitala produkter.

4. Under 2026–2027 utveckla och utöka resurserna för tjänsten Cybersäkerhetsrådgivningen så att verksamhetsutövare (såväl sådana som levererar som sådana som mottar digitala produkter) som har utmaningar med att uttolka eller tillämpa kraven i föreskrifterna, eller med att tillämpa metodstödet eller Leveranskedjekollen, eller på annat sätt har utmaningar i arbetet med att stärka säkerheten sina digitala leveranskedjor kan få tillgång till rådgivning av NCSC:s experter.

5. Under 2027–2028 inom ramen för den nationella Tänk säkert-kampanjen, såväl som via andra initiativ, informera verksamhetsutövare om existensen av, samt stödja verksamhetsutövare i tillämpningen av det utvecklade metodstödet och Leveranskedjekollen.

6. Under 2027–2028, bl.a. genom tjänsten Cybersäkerhetskollen, samla in uppgifter om vilka digitala leveranskedjor verksamhetsutövare som omfattas av Cybersäkerhetslagen[23] ingår i och utifrån de insamlade uppgifterna identifiera för samhället särskilt viktiga leverantörer av digitala produkter och de leveranskedjor de upprätthåller. Utifrån kartläggningen ta fram ett koncept för hur det nationella cybersäkerhetscentret vid incidenter hos sådana leverantörer proaktivt kan bistå leverantören i att informera mottagare av leverantörens digitala produkter om det inträffade, samt på vilka sätt, inklusive i termer av icke-linjära konsekvenser, som respektive mottagare kan förvänta sig att bli påverkad.

7. Under 2029 öva, och utifrån övningen, utvärdera och utveckla det framtagna konceptet för hur det nationella cybersäkerhetscentret vid incidenter hos sådana leverantörer proaktivt kan bistå leverantören i att informera mottagare av leverantörens digitala produkter.

8. Under 2027–2028 se över möjligheterna att inom ramen för Cybersäkerhetsrådgivningen och med stöd av den ovan nämnda kartläggningen ge råd och stöd till verksamhetsutövare inför och under upphandlingsprocesser i syfte att undvika att monoberoenden etableras.

9. Under 2028–2029 utvärdera och utifrån utvärderingen utveckla Metodstödet, Leveranskedjekollen samt Cybersäkerhetsrådgivningen i syfte att bidra med ytterligare nytta för relevanta verksamhetsutövare.

10. Under 2026–2029 delta i NIS Samarbetsgruppens arbete med samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor i enlighet med art. 22 respektive 21(3) i NIS 2-direktivet.

[23] I enlighet med Uppdrag till Myndigheten för samhällsskydd och beredskap att genomföra en kartläggning av digitala leveranskedjor och att ta fram en modell för uppföljning av digitala leveranskedjor (Fö2025/00390).

11. Under 2027 starta ett nytt underforum till NIS Samarbetsforum där frågor koppling till NIS Samarbetsgruppens arbete med samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor i enlighet med art. 22 respektive 21(3) i NIS 2-direktivet kan hanteras gemensamt.

Åtgärder som regeringen rekommenderas att vidta

1. Nationellt cybersäkerhetscenter får under 2026–2027 i uppdrag att upprätta en funktion med tillhörande tekniskt stöd som med en hög grad av automatisering kontinuerligt kan samla in uppgifter från verksamhetsutövare om deras digitala leveranskedjor för att därigenom möjliggöra ett effektivt genomförande av det nationella cybersäkerhetscentrets åtgärd nr. 6 ovan.

2. Statliga myndigheter under regeringen får 2028 i uppdrag att ansluta sig till funktionen och dess tekniska lösning så att Nationellt cybersäkerhetscenter på automatisk väg får in uppgifter om statliga myndigheters digitala leveranskedjor, vilket därigenom möjliggör ett effektivt genomförande av det nationella cybersäkerhetscentrets åtgärd nr. 6 ovan.

3. Nationellt cybersäkerhetscenter, Myndigheten för civilt försvar och andra berörda myndigheter som har uppdrag i frågor som rör utländska direktinvesteringar, samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor och upphandlingar får 2027 i uppdrag att etablera en samverkan och att ta fram ett förslag till en nationell plan för hur riskerna med monoberoenden och inlåsningseffekter ska hanteras och förebyggas, samt hur den digitala suveräniteten ska stärkas såväl nationellt som inom EU, inklusive nationella mål för vad som ska uppnås.

Åtgärder som verksamhetsutövare rekommenderas att vidta

1. Verksamhetsutövare som omfattas av Cybersäkerhetslagen ska följa Myndigheten för civilt försvars (och fr.o.m. den 1 juli 2026, Nationellt cybersäkerhetscenters) föreskrifter. Genom att följa föreskrifterna bedrivs en stor del av det systematiska cybersäkerhetsarbete som såväl leverantörer som mottagare av digitala produkter behöver bedriva. Genom att följa föreskrifterna ställer också mottagare av digitala produkter krav på sina leverantörer som medför att de, även om de inte själva omfattas av Cybersäkerhetslagen, ska bedriva ett systematiskt cybersäkerhetsarbete.

2. Verksamhetsutövare som omfattas av Cybersäkerhetslagen och verksamhetsutövare som är leverantörer av digitala produkter bör använda tjänsten Cybersäkerhetskollen. Om de bedriver ett systematiskt cybersäkerhetsarbete kommer de vid mätningar i Cybersäkerhetskollens fyra

ingående delar[24] (eller tre, om de inte har ot-system) uppnå minst nivå 3. För att lösa utmaningar med att etablera och upprätthålla ett systematiskt cybersäkerhetsarbete bör de också använda sig av tjänsterna Cybersäkerhetsrådgivningen respektive Metodstödet för systematiskt cybersäkerhetsarbete.

Indikatorer

Referenser

[24] Infosäkkollen, it-säkkollen, ot-säkkollen respektive leveranskedjekollen.

Cybersäker upphandling

Enligt NIS 2-direktivets artikel 7.2 b) Riktlinjer för att inkludera och specificera cybersäkerhetsrelaterade krav för IKT-produkter och IKT-tjänster vid offentlig upphandling, inbegripet vad gäller cybersäkerhetscertifiering, kryptering och användning av cybersäkerhetsprodukter med öppen källkod.

Definitioner och begrepp

Cybersäkerhetsprodukt: En IKT-produkt vars huvudsakliga syfte är att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.[25].

Cybersäkerhetscertifiering: Den europeiska ordningen för cybersäkerhetscertifiering vilken omfattar en vittomfattande uppsättning regler, tekniska krav, standarder och förfaranden som fastställs på unionsnivå och som tillämpas på certifiering eller bedömning av överensstämmelse av särskilda IKT-produkter, IKT-tjänster och IKT-processer. [26].

Funktionella säkerhetskrav: Krav som beskriver vilka säkerhetskrav en leverantör eller vilka säkerhetsfunktioner en produkt eller tjänst ska uppfylla utan att specificera hur dessa ska implementeras[27].

IKT-produkter: Produkter som används för elektronisk behandling, lagring eller överföring av information, exempelvis hårdvara och mjukvara för kommunikation, databehandling och informationshantering[28].

IKT-tjänster: En tjänst som helt eller huvudsakligen består i överföring, lagring, hämtning eller behandling av information via nätverks- och informationssystem[29]

It-upphandling: Upphandling av IKT-produkter eller IKT-tjänster[30].

Kriterietjänst: Sammanställning av krav med tillhörande information om dess användning[31].

Kryptering: Algoritm och nyckel för att säkerställa behörighet till information, att information inte förändrats, och att man kan lita på information[32].

---

[25] Inspiration från https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32019R0881 Artikel 2.1 och 2.12.
[26] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32019R0881 Artikel 2.9 (något justerad)
[27] Inspiration av: https://www.upphandlingsmyndigheten.se/inkopsprocessen/genomfor-upphandlingen/funktionskrav-i-upphandling/
[28] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32019R0881
[29] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32019R0881
[30] Härledd definition.
[31] Inspiration från `https://www.upphandlingsmyndigheten.se/kriterier/#om_kriterietjansten
[32] Inspiration från https://sv.wikipedia.org/wiki/Kryptering

Leverantörsdialog: En strukturerad dialog mellan en upphandlande organisation och potentiella leverantörer inför- eller under en upphandling[33].

Öppen källkod: Datorprogram vars källkod inte är proprietär utan är tillgänglig att använda, läsa, modifiera och vidaredistribuera[34].

Introduktion

Denna policy tar upp offentliga organisationers möjligheter och svårigheter att identifiera säkerhetskrav för IKT-produkter och IKT-tjänster vid offentlig upphandling. Policyn berör också vilket stöd som finns för att identifiera säkerhetskrav inklusive krav för cybersäkerhetscertifiering, kryptering och användning av cybersäkerhetsprodukter med öppen källkod. Policyn visar på det stöd som finns och behov av att förtydliga stödet kring hur säkerhetskrav identifieras och vilka säkerhetsåtgärder som behöver finnas i IKT-produkter och IKT-tjänster utifrån ställda säkerhetskrav. Stödet behövs både för upphandlande organisationer och leverantörer till dessa. Behoven av stöd som identifierats är bland annat kompetenshöjande insatser inom både upphandling av dessa produkter och tjänster samt inom cybersäkerhet. Det behöver också vara tydligare var stöd finns och att ett arbete med att ta fram en grunduppsättning säkerhetskrav i olika nivåer (gemensamma skyddsnivåer) för att underlätta dialogen mellan upphandlande organisationer och leverantörer skulle underlätta för aktörer i en upphandling.

Avgränsning

Policyn fokuserar på offentlig sektors upphandling av IKT-tjänster och IKT-produkter. Vi har därför avgränsat oss att ge exempel på existerande stöd och fokusera på några viktiga roller vid upphandlingar hos upphandlande organisationer samt behovet av stöd för dialoger mellan upphandlande och levererande organisation.

Nulägesbild

Informations- och kommunikationsteknologisektorn (IKT-sektorn) består av de företag vars verksamhet är inriktad på produktion av varor och tjänster som möjliggör elektronisk insamling, lagring, överföring, behandling och presentation av information. Det finns begränsat med statistik kring hur omfattande IKT-sektorn är i Sverige, men det bredare begreppet techsektorn som används mer informellt och inbegriper samma typer av produkter och tjänster, kan ge en fingervisning. I en rapport från Tech Sverige[35] uppges att techbranschens

[33] https://www.upphandlingsmyndigheten.se/inkopsprocessen/forbered-upphandling/tidig-dialog/dialogmoten-med-leverantorer/
[34] https://sv.wikipedia.org/wiki/%C3%96ppen_k%C3%A4llkod
[35] https://techsverige.se/app/uploads/2023/11/TECH-SVERIGE-RAPPORT-SVENSKA-TECHBRANSCHEN-2023.pdf

omsättning 2022 var över 1000 miljarder kronor och att dess bidrag till Sveriges BNP uppgick till ca 350 miljarder kronor eller 7,9 procent av BNP.

Det finns inte heller tillgänglig statistik som visar för hur mycket IKT-produkter och -tjänster upphandlas eller hur stor del av de offentliga affärerna som utgörs av dem. Totalt uppgår de offentliga upphandlingarna i Sverige till över 1000 miljarder kronor vilket motsvarar ca. 18,4 procent av BNP[36]. Inom EU finns över 250 000 upphandlande offentliga organisationer och ca. 14 procent av EU:s BNP läggs på offentlig upphandling, något som motsvarar ca 2 biljoner euro per år[37].

EU kommissionen uppmärksammar att det finns stor tillgång till information om offentlig sektors IKT-upphandlingar men att den är ostrukturerad och varierande avseende format och klassificeringar av informationen så det är svårt att undersöka statistiskt.[38]

Alla länder inom EU har motsvarigheter till den svenska regleringen om offentlig upphandling då regelverken bygger på samma EU-direktiv.[39] Regleringen är till för att gynna EU:s inre marknad och främja konkurrens, transparens, effektivitet och innovation inom hela unionen. Företag i ett medlemsland ska ha goda möjligheter till att göra affärer med offentliga organisationer i de andra medlemsländerna.

I Sverige regleras offentliga upphandlingar främst genom lagen om offentlig upphandling, (LOU).[40] Syftet med regleringen är att säkerställa att offentliga medel i Sverige används effektivt, transparent och att konkurrensen gynnas. Statliga myndigheter, regioner, kommuner och offentligt ägda bolag är alla skyldiga att följa LOU vid inköp av varor, tjänster och för byggentreprenad där kostnaderna beräknas överstiga vissa tröskelvärden. Det finns utöver LOU lagar för vissa inköp beroende på vem och vad som upphandlas. Dessa är lagen om upphandling på försvars- och säkerhetsområdet (LUFS)[41], lagen om upphandling inom vatten, energi, transporter och posttjänster (LUF)[42] samt lagen om upphandling av koncessioner (LUK)[43].

I färdplan för de offentliga affärerna[44] framgår att det är viktigt att offentlig sektor planerar sina inköp utifrån sina behov och identifiera vilka krav som ska ställas

[36] https://www.upphandlingsmyndigheten.se/nyheter/2025/upphandling-for-1-009-miljarder/
[37] https://single-market-economy.ec.europa.eu/single-market/public-procurement_en
[38] https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement/public-procurement-data-space-ppds_en
[39] Europaparlamentets och rådets direktiv 2014/24/EU
[40] LOU, SFS 2016:1145
[41] https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-20161145-om-offentlig-upphandling_sfs-2016-1145/
[42] https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-20161146-om-upphandling-inom_sfs-2016-1146/
[43] https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-20161147-om-upphandling-av-koncessioner_sfs-2016-1147/
[44] https://www.regeringen.se/contentassets/7ef58f17c4a14a6eb2ccd9b0ea5e4e84/fardplan-for-de-offentliga-affarerna-20252030.pdf

som en naturlig del av sin verksamhetsplanering. Det behöver också avsättas resurser med kompetens för att planera inköp och identifiera relevanta krav. Det framgår också att identifiera behov av cybersäkerhet och ställa krav på det vid inköp blir allt viktigare.

Cybersäkerhetsläget gällande upphandling i Sverige

Det finns ingen samlad statistik över hur många offentliga upphandlingar som ställer krav på cybersäkerhet vid it-upphandlingar och inte heller om de krav på cybersäkerhet som ställts resulterar i den säkerhet som kravställts. Därmed saknas också analyser av vilka eventuella effekter ställda cybersäkerhetskrav får på till exempel säkerheten i produkter och tjänster eller på företagens möjligheter att kvalificera sig som anbudsgivare genom att leverera produkter och tjänster som uppfyller ställda säkerhetskrav. Tendiums senaste rapport (2024)[45] visar dock en ökning i förekomsten av ordet "cybersäkerhet" i underlag för it-upphandlingar de senaste åren. Detta ger en indikation på att krav på säkerhet i it-upphandlingar ökar. Undersökningen har inte undersökt förekomsten av närliggande begrepp så som informationssäkerhet eller it-säkerhet.

Myndigheten för samhällsskydd och beredskap (MSB)[46] genomför återkommande mätningar med verktyget Cybersäkerhetskollen[47]. Ett av de områden som mäts är hur organisationer arbetar med att ställa och följa upp krav på säkerhet vid inköp och utkontrakteringar. Mätningar med stöd av Cybersäkerhetskollen har genomförts vid fyra tillfällen mellan år 2021–2025. Verktyget riktar sig i första hand till organisationer inom offentlig förvaltning och företag som omfattas av NIS-regleringen men alla organisationer uppmuntras att använda verktyget som stöd i sitt informations- och cybersäkerhetsarbete och att delta i de återkommande mätningarna. Utifrån inrapporterade resultat[48] sammanställer MSB en nationell lägesbild av det systematiska cybersäkerhetsarbetet. Upphandling var ett av de områden där minst förbättring syntes mellan mättillfällena 2023 och 2024. I mätningen 2024 uppgav 40 procent av kommunerna att de saknat arbetssätt för att säkerställa informationssäkerhet vid upphandling under de senaste två åren, ca. 75 procent av regionerna hade inte följt upp om krav som ställts vid upphandlingar varit tillräckliga eller om leverantörer uppfyllt ställda krav. En stor majoritet av myndigheterna hade inte följt upp eller utvärderat sina arbetssätt vid upphandling för att säkerställa att leverantörerna omhändertagit informations- och cybersäkerhetskrav i tillräcklig omfattning.

[45] https://upphandling24.se/wp-content/uploads/2025/05/Rapport-Offentlig-upphandling-2024-Tendium.pdf
[46] Från om med 1 januari 2026 Myndigheten för civilt försvar.
[47] https://www.msb.se/sv/publikationer/resultatredovisning-av-cybersakerhetskollen-2024--det-systematiska-cybersakerhetsarbetet-i-den-offentliga-forvaltningen/
[48] https://rib.msb.se/filer/pdf/30971.pdf

Vilka svårigheter organisationer upplever med det systematiska informations- och cybersäkerhetsarbetet får Myndigheten för civilt försvar bland annat via frågor som ställs till cybersäkerhetsrådgivningen, andra delar av myndigheten, frågor och önskemål om föredrag, genom erfarenhetsutbyte i olika målgruppsanpassade nätverk eller via undersökningar[49].

Nationellt cybersäkerhetscenter (NCSC) lyfter i rapporten ”Cybersäkerhet i Sverige 2024” att otillräcklig kravställning gällande cybersäkerhet är ett problem för cybersäkerheten hos enskilda organisationer och samhället i stort samt att det krävs relevant kompetens inom cybersäkerhet både vid upphandling av produkter och tjänster samt vid utkontraktering av it-infrastruktur. NCSC nämner i rapporten att tydliga avtal och krav som utgår från relevanta standarder som viktiga områden att arbeta med för att möta problemen. Man lyfter också risker förknippade med att många underleverantörer inte bedriver ett tillräckligt bra cybersäkerhetsarbete i förhållande till vad de levererar.

Stöd och vägledning vid upphandling

Det finns många aktörer som erbjuder stöd och information om upphandling generellt, för offentliga upphandlingar och stöd kopplat till upphandlingar av IKT-produkter och IKT-tjänster både för upphandlande och levererande sida. Utbudet är stort och spritt bland många aktörer. Det finns också många aktörer som erbjuder stöd för informations- och cybersäkerhet. Nedan följer en övergripande sammanställning av dessa.

Upphandlingsmyndigheten erbjuder vägledningar, mallar, stöd gällande inköpsprocessen, bland annat stöd kring ledning av en inköpsorganisation, en direktupphandlingsguide, stöd till levererande sida med mera.[50] De erbjuder också en tjänst för att underlätta kravställningen för hållbarhetskriterier med fokus på miljömässig och social hållbarhet, en kriterietjänst.[51] Myndigheten erbjuder också en frågeportal dit vem som helst är välkommen att höra av sig med frågor som rör både upphandling generellt och mer specifikt IKT-upphandling. Användare kan både ställa egna frågor och ta del av andras frågor och myndighetens svar. Det finns också temasidor om bland annat informationssäkerhet vid upphandling[52] och en introduktion till säkerhetsskydd[53]. I december 2025 fick Upphandlingsmyndigheten bland annat i uppdrag att inrätta ett forum som ska

[49] Slutrapport Behovsanalys informationssäkerhet - Upplevda hinder vid systematiskt informationssäkerhetsarbete (år 2023) diarienummer MSB 2025–13424
[50] https://www.upphandlingsmyndigheten.se
[51] https://www.upphandlingsmyndigheten.se/kriterier/
[52] https://www.upphandlingsmyndigheten.se/regler-och-lagstiftning/andra-regler-som-kan-bli-aktuella/informationssakerhet-vid-upphandling/
[53] https://www.upphandlingsmyndigheten.se/regler-och-lagstiftning/andra-regler-som-kan-bli-aktuella/sakerhetsskyddad-upphandling/sakerhetsskydd-intro/

samordna upphandlingsstöd kopplat till inköpskategorin informationsteknik och bidra till att främja offentlig sektors it-inköp[54].

Konkurrensverket är tillsynsmyndigheten för offentlig upphandling. Hos dem kan man bland annat hitta en databas med domar i upphandlingsmål, en ordlista med upphandlingstermer, myndighetens ställningstaganden och en vägledning om undantaget för tekniska skäl.[55] På deras hemsida finns även temasidor om bland annat konkurrens och upphandling i kristider.

Kammarkollegiet genomför upphandlingar och erbjuder stöd vid avrop från ramavtal genom Statens inköpscentral. På sin hemsida avropa.se[56] erbjuder de information och stöd till både upphandlande och levererande sida om ramavtal, hur anbud lämnas och hur man avropar från ramavtalen.

Adda är Sveriges kommuner och regioners, SKR:s, inköpscentral. De erbjuder information och stöd till de organisationer som kan nyttja deras ramavtal samt de företag som vill leverera på ramavtalen[57]. De erbjuder också information kring försörjningsberedskap och upphandling[58]. SKR tillhandahåller också Klassa, ett verktyg som bland annat hjälper organisationer att ställa krav på säkerhet vid upphandlingar.[59]

Myndigheten för digital förvaltning (Digg) erbjuder olika stödmaterial som kan vara relevanta vid upphandlings av IKT-produkter och IKT-tjänster. Bland annat stödjer de med förslag på kravtexter till upphandlingar av it-system och digitala tjänster[60] och ger ut rekommendationer för upphandling av data[61].

E-hälsomyndigheten tillhandahåller kunskapsstöd för e-hälsa om vänder sig till kommunal hälso- och sjukvård samt socialtjänst. Stödet är en sammanställning av bland annat material för att identifiera behov av säkerhet vid innovation, utveckling och upphandling av system.[62]

[54] https://www.regeringen.se/regeringsuppdrag/2025/12/uppdrag-till-upphandlingsmyndigheten-att-framja-och-folja-upp-genomforandet-av-fardplanen-for-de-offentliga-affarerna/
[55] https://www.konkurrensverket.se/upphandling/
[56] https://www.avropa.se/
[57] https://www.adda.se/upphandling-och-ramavtal/
[58] https://www.adda.se/upphandling-och-ramavtal/forsorjningsberedskap/
[59] https://klassa.skr.se/
[60] https://www.digg.se/kunskap-och-stod/oppna-och-delade-data/offentliga-aktorer/rekommendationer-for-upphandling-av-data/forslag-pa-kravtexter-till-upphandlingar-av-it-system-och-digitala-tjanster
[61] https://www.digg.se/kunskap-och-stod/oppna-och-delade-data/offentliga-aktorer/rekommendationer-for-upphandling-av-data
[62] https://www.ehalsomyndigheten.se/yrkesverksam/e-halsostod-till-kommuner/kunskapsstod-for-e-halsa/sok-bland-kunskapsstoden-for-e-halsa/

Säkerhetspolisen erbjuder bland annat en vägledning om skyldigheter vid exponering av säkerhetsskyddad verksamhet[63] och vägledningar om säkerhetsskydd.[64]

Även Europeiska byrån för nät- och informationssäkerhet (Enisa), erbjuder stödmaterial som kan vara relevant vid upphandling av IKT-produkter och IKT-tjänster, bland annat Security Guide for ICT Procurement[65] och Good Practices for Supply Chain Cybersecurity[66].

Myndigheten för civilt försvar tillhandahåller en mängd olika stöd i arbetet med informations- och cybersäkerhet. Flera av dessa ger stöd för kravställning av IKT-produkter och IKT-tjänster genom att ge kravställande organisationer förutsättningar för att vid en upphandling ställa säkerhetskrav som uppfyller det behov av säkerhetsåtgärder som informationen som behandlas och systemen som behandlar informationen behöver. Ett urval av dessa är:

- Vägledningen ”Upphandla informationssäkert” ger stöd i att identifiera de krav som behöver ställas beroende på vilken information som leverantören får tillgång till.[67]
- Metodstöd för systematiskt informationssäkerhetsarbete ger stöd för hur ett informationssäkerhetsarbete i en organisation bör bedrivas och därmed vilka krav som bör ställas på en leverantörs informationssäkerhetsarbete.[68]
- Vägledningen säkerhet i informationssystem stödjer med krav som kan behöva ställas på egna och en leverantörs IKT-produkt eller IKT-tjänst.[69]
- Publikationerna Grundläggande säkerhet i cyberfysiska system[70] och Ökad säkerhet i industriella informations- och styrsystem vilken ger stöd i att förstå de särskilt krav som gäller organisationens ot-miljö och därmed bör ställas vid upphandling av IKT-produkter och IKT-tjänster som är eller kommunicerar med cyberfysiska system[71]
- Vägledningen för fysisk informationssäkerhet i it-utrymmen[72] är framtagen av MSB tillsammans med riksarkivet och beskriver hur man kan identifiera

63 https://www.sakerhetspolisen.se/download/18.3222e1b7187a064b070e6/1683815514604/Skyldighet%20vid%20exponering%20av%20sa%CC%88kerhetska%CC%88nslig%20verksamhet_anpassad.pdf
64 https://sakerhetspolisen.se/sakerhetsskydd/vagledningar-sakerhetsskydd.html
65 https://www.enisa.europa.eu/publications/security-guide-for-ict-procurement
66 https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practices%20for%20Supply%20Chain%20Cybersecurity.pdf
67 https://rib.msb.se/filer/pdf/28742.pdf
68 https://metodstod-informationssakerhet.msb.se/
69 https://www.msb.se/sv/publikationer/vagledning--sakerhetsatgarder-i-informationssystem/
70 https://www.msb.se/sv/publikationer/grundlaggande-sakerhet-i-cyberfysiska-system--vagledning/
71 https://www.msb.se/sv/publikationer/vagledning-till-okad-sakerhet-i-industriella-informations--och-styrsystem/
72 https://www.msb.se/sv/publikationer/vagledning-for-fysisk-informationssakerhet-i-it-utrymmen/

vilka krav på fysiskt skydd som kan behöva ställas på olika utrymmen där system finns (it-utrymmen).

Myndigheten för civilt försvar erbjuder också tjänsten Cybersäkerhetsrådgivningen[73] med personlig kostnadsfri rådgivning om frågor kring förebyggande informations- och cybersäkerhetsarbete som ett komplement till övrigt stöd. Dessutom kan organisationer skicka in sina resultat från Cybersäkerhetskollen[74], och få återkoppling på utvecklingsområden för att förbättra sin informations-och cybersäkerhet.

Bland övriga aktörer som erbjuder stöd finns bland annat Stöldskyddsföreningen som erbjuder informationsmaterial gällande cybersäkerhet och grundläggande it-säkerhet[75] samt tjänsten Säkerhetskollen för företag[76]. Svenska institutet för standarder[77] erbjuder en mängd standarder inom informations- och cybersäkerhet som kan vara till stöd vid kravställning.

Det finns också många företag och organisationer som erbjuder utbildningar av olika längd och på olika nivå inom upphandling, offentlig upphandling och offentlig upphandling med specifikt digitalisering eller säkerhet i fokus. Exempel på längre utbildningar är Företagsuniversitets kurser upphandling av digitaliserings- och it-lösningar[78] och säkerhetsskyddad upphandling[79]. Det finns också leverantörer av kurser för att bli kvalificerad it-upphandlare, certifierad it-upphandlare, lära sig mer om säkerhetsskyddad upphandling eller robusta it-avtal och företag som erbjuder korta kurser på temat.

Nationella krav på cybersäkerhet

Det finns flera lagar och förordningar med tillhörande föreskrifter som ställer krav på att skydda den information som en organisation ansvarar över. Regleringen omfattar antingen skyddet av informationsbehandling generellt, fokuserar på en viss information eller en viss verksamhet och den informationsbehandling som förekommer där. Kraven i de olika regleringarna kan vara generella, exempelvis att

[73] https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/arbeta-systematiskt-med-informationssakerhet-och-cybersakerhet/radgivningstjanst/
[74] https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/arbeta-systematiskt-med-informationssakerhet-och-cybersakerhet/cybersakerhetskollen/
[75] https://www.stoldskyddsforeningen.se/butik/foretag/ssf-normer/cybersakerhet/ssf-1101-utg-2-ssf-cybersakerhet-basniva-grundlaggande-it-sakerhet/?srsltid=AfmBOoqQ31Le8chmXc-KatB9EOvYfl9LJEjNjaaSF6_SDbAklpfrQpE4
[76] https://sakerhetskollen.se/foretag
[77] https://www.sis.se/
[78] https://www.foretagsuniversitetet.se/yh-utbildningar/Upphandling-av-digitaliserings-och-IT-loesningar?gad_source=1&gad_campaignid=19700191138&gclid=EAIaIQobChMI7oXaiKKNkgMVqIyRBR0eexGdEAAYASAAEgJd9fD_BwE
[79] https://www.foretagsuniversitetet.se/yh-utbildningar/Saekerhetsskyddad-upphandling?gad_source=1&gad_campaignid=9982434168&gclid=EAIaIQobChMIjtKqmqONkgMVBxiiAx2rJgI5EAAYAiAAEgKsxfD_BwE

informationsbehandlingen ska skyddas tillräckligt eller så ställer regleringen specifika krav på olika säkerhetsåtgärder som behöver vidtas för att ge ett tillräckligt skydd.

Säkerhetsskyddslagen ställer bland annat krav på att identifiera var säkerhetsskyddade uppgifter behandlas och att informationssystem som behandlar dessa ska vara godkända för sådan behandling. Säkerhetspolisen ger ut föreskrifter[80] och vägledningar om säkerhetsskydd, bland annat om hur information ska skyddas i sin vägledning om informationssäkerhet[81] .

EU:s allmänna dataskyddsförordning GDPR[82] ställer krav på att tillse ett tillräckligt skydd av personuppgifter. I detta ingår att identifiera personuppgifter och genomföra konsekvensanalyser för vilken skada ett otillräckligt skydd kan få för de personer vars uppgifter organisationen behandlar. För skyddet av personuppgifter ger integritetsskyddsmyndigheten[83] ut vägledningar och erbjuder utbildningar och rådgivning till olika målgrupper bland annat personuppgiftsansvariga och personuppgiftsbiträden.

I Sverige införs EU:s NIS 2-direktiv[84] bland annat genom cybersäkerhetslagen (2025:1506)[85]. Cybersäkerhetslagen ställer krav på organisatoriska, tekniska och driftrelaterade säkerhetsåtgärder samt de säkerhetsåtgärder som behövs för att skydda den fysiska miljön där system som behandlar informationen finns. Myndigheten för civilt försvar kommer att genom föreskrifter[86] bland annat förtydliga innebörden av de säkerhetsåtgärder som beskrivs i cybersäkerhetslagen.

För statliga myndigheter ställs krav på informationssäkerhet utifrån Beredskapsförordningen (2022:524) och MSB har givit ut föreskrifter (MSBFS 2020:6 och 2020:7) för att förtydliga kraven.

Exempel på andra föreskrifter som ställer krav på organisationer inom offentlig sektor är Socialstyrelsens föreskrifter[87] med bland annat krav på säkerhet vid journalföring och behandling av personuppgifter i hälso- och sjukvård.

Annan reglering så som offentlighets och sekretesslagen (2009:400) ställer indirekt krav på säkerhetsåtgärder för information som skyddas av sekretess. Lagen om

[80] https://www.sakerhetspolisen.se/download/18.650ed51617f9c29b5522c6/1649764927944/Sakerhetspolisens_foreskrifter_om_sakerhetsskydd_PMFS_2022_1.pdf
[81] https://www.sakerhetspolisen.se/download/18.3752daf918b497112712b/1698133722307/Informationssa%CC%88kerhet_anpassad.pdf
[82] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679
[83] https://www.imy.se/
[84] https://eur-lex.europa.eu/legal-content/sv/TXT/?uri=CELEX%3A32022L2555
[85] https://svenskforfattningssamling.se/sites/default/files/sfs/2025-12/SFS2025-1506.pdf
[86] https://www.regeringen.se/regeringsuppdrag/2025/09/uppdrag-till-myndigheten-for-samhallsskydd-och-beredskap-att-forbereda-genomforandet-av-nis-2-direktivet/
[87] https://www.socialstyrelsen.se/kunskapsstod-och-regler/regler-och-riktlinjer/foreskrifter-och-allmanna-rad/konsoliderade-foreskrifter/201640-om-journalforing-och-behandling-av-personuppgifter-i-halso--och-sjukvarden/

elektroniska kommunikationer (2022:482) ställer krav på att digitala kommunikationstjänster bland annat ska vara tillgängliga och i övrigt skyddade mot hot och incidenter.

Cybersäkerhetscertifiering, produktdeklarationer och andra krav

Flera initiativ finns för att hjälpa köpare att välja säkrare IKT-produkter och IKT-tjänster och för leverantörer att visa vilket skydd deras produkter och tjänster har.

Cybersäkerhetscertifieringar

Det finns och utvecklas löpande nya EU-gemensamma regler förcybersäkerhets-certifiering av olika IKT-produkter och IKT-tjänster utifrån EU:s ramverk för cybersäkerhetscertifiering, i enlighet med EU:s Cybersäkerhetsförordning[88]. I Sverige har Försvarets materielverk (FMV) rollen som nationell myndighet för certifiering inom cybersäkerhet. Certifikat som utfärdats för en IKT-produkt, IKT-tjänst eller IKT-process enligt ett europeiskt lands cybersäkerhetscertifiering är giltiga i hela unionen.

Certifieringarna underlättar för kunder och användare att välja produkter och tjänster med rätt nivå av säkerhet utifrån sina behov och krav.

Det är för närvarande frivilligt att använda IKT-produkter och IKT-tjänster med europeiska certifikat. De kan dock komma att bli obligatoriska inom, till exempel vissa sektorer enligt NIS 2-direktivet och för vissa it-produkter utifrån EU:s Cyberresiliensförordning.[89]

Ytterligare europeiska certifieringsordningar är under utveckling, bland annat för molntjänster och produkter med digitala element, vilket på sikt kommer att påverka möjligheten att ställa krav på certifierade produkter och tjänster samt att det finns certifierade produkter som utbud i tillexempel offentligt upphandlade tjänster.

Produktdeklarationer

I EU:s Cyberresiliensförordning[90]ställs cybersäkerhetskrav på produkter med digitala element och att tillverkare upprättar en programvarudeklaration över de komponenter som ingår i en produkt. Syftet är att underlätta identifiering av produkter med sårbarheter och identifiera risker vid användning av produkten. Deklarationerna möjliggör en bättre förståelse för risker i leveranskedjan hos de som tillverkar, köper eller tillhandahåller programvara.

[88] https://eur-lex.europa.eu/SV/legal-content/summary/the-eu-cybersecurity-act.html
[89] Cyberresiliensförordningen (EU 2024/2847)
[90] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=OJ:L_202402847

Godkända IKT-produkter inom Nato

Också Nato erbjuder ett certifieringsförfarande för IKT-produkter. Natos Information Assurance Product Catalogue (NIAPC) är ett register över IKT-produkter och skyddsprofiler som uppfyller Natos säkerhetskrav. För att en IKT-produkt godkänd av Nato också ska anses godkända i EU krävs att FMV godkänner produkterna enligt EU:s regelverk.

Krav på kryptering

Kryptering är en viktig säkerhetsåtgärd för att skydda information i digitala miljöer. Vid användning av kryptering rekommenderar Nationellt cybersäkerhetscenter (NCSC)[91] att endast standardiserade algoritmer användas, såsom NIST FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard, NIST FIPS 204 Module-Lattice-Based Digital Signature Standard och NIST FIPS 205 Stateless Hash-Based Digital Signature Standard.

För att hantera hotet från kvantdatorer mot säkerheten i befintliga krypteringslösningar har EU tagit fram en färdplan i två delar för att uppnå kvantsäkrad kryptografi inom unionen[92]. Den första delen innehåller konkreta råd om aktiviteter som behöver vidtas av organisationer som använder kryptering för att förbereda sig inför att valda krypteringslösningar inte längre bedöms som säkra. Den andra delen kommer att innehålla bland annat mer detaljerade och utförliga rekommendationer rörande algoritmer.

Krav på cybersäkerhetsprodukter med öppen källkod

I skälen till EU:s Cyberresiliensförordning[93] anges att hård- och programvara som tillgängliggörs för den europeiska marknaden ska utvecklas så att säkerhet omhändertas i produktens hela livslängd. Detta för att minska antalet sårbarheter i IKT-produkter. I artikel 13 ställs krav på stor riskmedvetenhet när programvara med fri och öppen källkod används i IKT-produkter. Det ska finnas dokumentation om hur programvara med öppen källkod har utvecklats för att omhänderta ställda säkerhetskrav. Detta för att underlätta bedömningen av säkerheten i ingående programvaror vid val av IKT-produkter.

Digg har publicerat vägledningen Policy för anskaffning samt utveckling av programvara[94]där offentliga aktörer uppmanas att ha programvara med öppen källkod som förstahandsval vid upphandlingar. Policyn detaljeras i Riktlinjer för utveckling och publicering av öppen programvara.[95] Det är i övrigt ont om stöd för att närmare förstå vad en organisation behöver beakta vid utveckling av programvara eller val av produkter med öppen källkod. Det finns heller ingen

[91] https://www.ncsc.se/siteassets/publikationer/rekommendationer-for-overgangen-till-kvantsaker-kryptografi.pdf
[92] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=OJ:L_202401101
[93] Cyberresiliensförordningen (EU 2024/2847)
[94] Policy för anskaffning samt utveckling av programvara (Digg, 2022)
[95] Riktlinjer för utveckling och publicering av öppen programvara (Digg, 2022)

statistik som visar på hur ofta krav på produkter och tjänster med öppen källkod ställs i offentliga upphandlingar, vilka krav som ställs eller sådana tjänster väljs och hur säkerheten i dessa produkter ser ut över tid.

Om det är skillnad mellan IKT-produkter generellt och cybersäkerhetsprodukter specifikt gällande kravställning av cybersäkerhet, utbudet av produkter som uppfyller både säkerhetskrav och funktion samt hur dessa produkter förhåller sig till produkter utan öppen källkod gällande säkerhet under produktens livslängd är också oklart.

Relaterade svenska initiativ för att öka cybersäkerheten

Regeringen beslutade 2024 om förordningen om samordnad och säker statlig it-drift[96] för att ge statliga myndigheter tillgång till moderna, säkra och kostnadseffektiva it-verktyg och it-tjänster. Syftet är att möjliggöra för statliga myndigheter en driftmiljö där de kan bedriva sina verksamheter på ett säkert sätt då verktygen och tjänsterna omhändertar risker som utgår från hela hotskalan.

I betänkandet från Interoperabilitetsutredningen[97] lyfts att nuvarande arbetssätt där organisationer i den offentliga förvaltningen skyddar sin information utifrån organisationens egna förutsättningar och behov inte omhändertar samhällets behov av säkerhet vid informationsdelning. Det arbetssättet försvårar datautbyte och medför att samhällets övergripande behov av information och skydd för informationen blir svårt att omhänderta. Utredningen föreslår därför att det tas fram gemensamma skyddsnivåer. De gemensamma skyddsnivåerna innehåller säkerhetsåtgärder med olika styrkor beroende på nivå. Sådana gemensamma skyddsnivåer skulle underlätta dialogen vid utbyte av information mellan olika aktörer genom att de skulle kunna användas både för att kommunicera behov av säkerhetsåtgärder till den som är eventuell mottagare av informationen och för eventuell mottagare att visa vilket skydd denne kan ge informationen vid datadelning.

Dessa nivåer skulle också kunna användas på liknande sätt vid upphandlingar där beställande organisation beskriver vilken skyddsnivå alla eller majoriteten av säkerhetskrav ligger på och potentiella leverantörer vars produkter eller tjänster uppfyller efterfrågad skyddsnivå kan visa på det. Beställare och leverantör skulle då kunna fokusera på att omhänderta eventuella ytterligare säkerhetsåtgärder utöver de i skyddsnivån som behöver tillgodoses utifrån den specifika

[96] https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-20241005-om-samordnad-och-saker_sfs-2024-1005/
[97] https://www.regeringen.se/contentassets/6866c386b0ec492c8171c92c9c8922cf/en-reform-for-datadelning-sou-202396.pdf

informationsbehandlingen som IKT-produkten eller IKT-tjänsten ska användas för.

Ett annat initiativ är Sveriges digitala infrastruktur (Ena). Ena byggs utifrån gemensamma standarder och för att upprätthålla hög säkerhet för att säkerställa effektiv datadelning, skapa en gemensam väg in till den offentliga förvaltningen samt främja samverkan mellan offentliga och privata organisationer. Infrastrukturen byggs också för att möjliggöra användning av AI- och datadriven utveckling. Arbetet samordnas av Digg.

Inom ramen för NCSC[98] pågår ett arbete med att ta fram en nationell modell som ska utgöra en gemensam plattform för det systematiska informationssäkerhetsarbetet genom att samordna och samla regelverk, metoder, verktyg, utbildningar med mera på ett lättillgängligt sätt.

Flera offentliga organisationer, fram för allt större organisationer med stort it-beroende arbetar systematiskt med att identifiera säkerhetskrav för att skydda information som de ansvarar för både om de behandlar den själva eller utkontrakterar den. Organisationer med hög grad av utkontraktering har i många fall för sina säkerhetskrav också formulerat upphandlingskrav för att underlätta arbetet och följer upp och förbättrar dessa krav över tid.

Som utgångspunkt för arbetet med att identifiera cybersäkerhetkrav för upphandling av IKT-produkter och IKT-tjänster finns förutom krav i regleringar också organisationer med lång erfarenhet av att ställa och följa upp cybersäkerhetskrav för olika IKT-produkter och IKT-tjänster. Exempel på sådana organisationer som tagit egna initiativ att erbjuda sådana underlag är upphandlingscentralen och Internetstiftelsen. Vi vet sedan tidigare att det finns organisationer som kommit mycket långt i att ta fram cybersäkerhetskrav och följa upp att de fungerar utifrån sin verksamhet Vi bedömer att det finns en stor erfarenhet hos offentlig sektor som kan återanvändas i arbetet med att ta fram gemensamma cybersäkerhetskrav och strukturera dem i skyddsnivåer.

Analys av nuläget

Det är positivt att det idag finns många initiativ från olika håll för att underlätta för offentliga organisationer att ställa cybersäkerhetsrelaterade krav i upphandlingar av IKT-produkter och IKT-tjänster. Det är också positivt att det finns förslag och påbörjade initiativ för att samordna cybersäkerhetskrav för att underlätta kravställningen för offentlig förvaltning och samtidigt underlätta för leverantörer av IKT-produkter och IKT-tjänster att utveckla sina produkter och tjänster mot enhetliga säkerhetskrav. Samtidigt visar bland annat statistik från Cybersäkerhetskollen att upphandling är ett område där utvecklingen kring stärkt

[98] Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022 (Ju2018/03737/SSK)

cybersäkerhet inte går i den takt som behövs. Några av de utmaningar som finns är:

1. Många verksamheter inom offentlig sektor som genomför it-upphandlingar saknar tillräckligt med resurser som har adekvat upphandlings- och cybersäkerhetskompetens. Konsekvenserna av bristande resurser och kompetens blir it-upphandlingar som inte ställer lämpliga, tillräckliga eller träffsäkra krav vilket i sin tur kan leda till bristande säkerhet i skyddet av informationen och de IKT-produkter och IKT-tjänster som behandlar informationen eller att onödigt höga krav på säkerhet ställs med höga kostnader till följd. En av de bakomliggande orsakerna är att ledningar inte förstått behovet av att avsätta resurser för att anskaffa de IKT-produkter och IKT-tjänster som verksamheterna behöver för att kunna bedrivas på ett säkert och effektivt sätt. En annan orsak är den snabba digitaliseringen som skapat behov av att upphandla säkra it-system och it-tjänster i en högre takt än det finns resurser mer rätt kompetens tillgängliga. Bristen gäller både personal med upphandlingskompetens och specialister som har kunskap att identifiera vilka säkerhetskrav som behöver ställas på olika IKT-produkter och IKT-tjänster och hur dessa bör följas upp.
2. Stödet för kravställning vid upphandling är spritt och ges ut av en mängd olika aktörer, vilket gör det svårt att få en korrekt, komplett och uppdaterad bild av vilket stöd som är aktuellt och relevant. Det kan därför vara svårt att hitta stöd som fungerar utifrån den egna verksamhetens behov och förutsättningar även i de fall ett sådant stöd finns. Orsakerna handlar om olika stödgivares mandat, uppdrag, målgrupp och förmåga att upprätthålla kvalitén i stödmaterialet samt bristande samverkan eller kommunikation mellan stödgivare och mellan stödgivare och den kravställande organisationen. Konsekvensen blir att relevant stöd inte används i den omfattning det skulle kunna och därmed inte skapar önskad effekt. Det kan också innebära att föråldrat eller felaktigt stöd används vilket leder till att organisationen inte ställer rätt krav utifrån sina behov.
3. Förmågan att följa upp ställda krav i avtal och att dessa fått den effekt på säkerhet som var syftet saknas hos många upphandlande organisationer. De bakomliggande orsakerna handlar om begränsade resurser med rätt kompetens för att genomföra offentlig upphandling men också brister i strategisk planering av behov av IKT-produkter och IKT-tjänster samt otillräcklig avtalsuppföljning. Konsekvensen blir osäkerhet kring att produkter och tjänster möter de krav som ställts eller att organisationen beslutar att utan att kontrollera lita på att leverantören förstått och uppfyller de krav som ställts.
4. Det finns initiativ för att ta fram nationellt gemensamma säkerhetskrav och strukturera dem i skyddsnivåer som stöd för organisationer att ställa

krav och leverantörer att utveckla IKT-produkter och IKT-tjänster som uppfyller dessa krav men flera av initiativen har inte genomförts. Konsekvenserna blir att organisationer som borde utveckla sin förmåga att ställa tillräckliga och träffsäkra funktionella säkerhetskrav avvaktar eller gör det bästa de kan med de resurser, kompetenser och erfarenheter de har. Orsaken till att gemensamma skyddsnivåer inte utvecklas kan vara att det kostnaden för bristande säkerhet, liksom vinster som görs genom digitalisering ses som den enskilde organisationens ansvar och möjlighet. Samhällets kostnad för bristande säkerhet i IKT-produkter och IKT-tjänster liksom hur gemensamma säkerhetskrav i skyddsnivåer skulle påverka samhällets kostnader för it-incidenter inte är tillräckligt utredd.

Målbild 2029

År 2029 avsätter offentlig sektor när de upphandlar IKT-produkter och IKT-tjänster tillräckligt med egna resurser, eller har tillgång till resurser, med den kompetens som behövs för att identifiera tillräckliga och träffsäkra funktionella säkerhetskrav vid upphandlingar av dessa produkter och tjänster.

År 2029 är det lätt för upphandlande organisationer och leverantörer till dessa att hitta relevant stöd kring cybersäkerhet i offentlig upphandling och hur kravställning av cybersäkerhet ser ut. Upphandlingsmyndigheten erbjuder, i samverkan med NCSC målgruppsanpassat stödmaterial för att ställa cybersäkerhetskrav till offentliga organisationers upphandlare, beställande verksamhet, samt informations- och cybersäkerhetsspecialister att förstå sin roll vid upphandling av IKT-produkter och IKT-tjänster. Samtidigt erbjuder NCSC kompletterande stöd till informations- och cybersäkerhetsspecialister inom offentlig sektor så att de kan stötta i upphandlingsprocessen kring vilka säkerhetskrav som behöver ställas och uppfyllas utifrån verksamhetens behov av IKT-produkter och IKT-tjänster. I stödet framgår också när offentlig sektor ska eller bör ställa krav på IKT-produkter och IKT-tjänster med cybersäkerhetscertifiering, vilken nivån på kryptering som ska eller bör erbjudas av produkter och tjänster samt när användning av cybersäkerhetsprodukter med öppen källkod ska eller bör användas och vilka säkerhetskrav som dessa behöver uppfylla. Det finns också stöd till leverantörer av IKT-produkter och IKT-tjänster att förstå innebörden av ställda krav så det finns leverantörer som kan möta offentlig sektors behov.

År 2029 följer offentliga organisationer upp hur väl ställda krav i avtal uppfyller behovet av säkerhet och har kunskap att omhänderta resultatet av sådan uppföljning genom dialog med leverantör om resultatet av uppföljningen visar på ett sådant behov. Organisationerna använder också lärdomar från uppföljningen till att förbättra sitt arbete med att ställa adekvata och tillräckliga cybersäkerhetskrav vid it-upphandling.

År 2029 arbetar Upphandlingsmyndigheten med stöd av NCSC med att erbjuda gemensamma cybersäkerhetskrav i nivåer för att underlätta för upphandlande organisationer att identifiera och välja adekvata och tillräckliga säkerhetskrav. Kraven hjälper också leverantörer att utveckla IKT-produkter och IKT-tjänster som uppfyller offentlig sektors behov. År 2029 har också arbetet med att ta fram ramavtal för ett antal IKT-produkter och IKT-tjänster utifrån de gemensamma säkerhetskraven i nivåer påbörjats.

Åtgärder för att uppnå målbilden

1. Upphandlingsmyndigheten har från 2027 ett uppdrag att med bistånd från NCSC och Säkerhetspolisen erbjuda ett upphandlingsstöd för att öka förståelsen för och kompetens hos ledningar i offentlig sektor om behovet av resurser vid upphandling av IKT-produkter och IKT-tjänster.

2. Upphandlingsmyndigheten har från 2027 ett uppdrag att utveckla och förvalta målgruppsanpassat upphandlingsstöd med cybersäkerhetskrav till upphandlande organisationer och potentiella leverantörer i den offentliga affären. Det finns också uppdrag att NCSC ska bidra till Upphandlingsmyndighetens arbete med stöd till målgrupperna upphandlare, verksamhet och informations- och cybersäkerhetsspecialister gällande att identifiera adekvata och tillräckliga cybersäkerhetskrav. I uppdraget ingår att erbjuda stöd för en både upphandlande organisationer och leverantörer i att genomföra värdeskapande leverantörsdialoger för dessa produkter och tjänster. I samverkan mellan Upphandlingsmyndigheten och NCSC ingår att NCSC analyserar det stöd för informations- och cybersäkerhetsspecialister som redan erbjuds för att säkerställa att stödet är tillräckligt för att offentlig sektor ska kunna identifiera sina risker och behov av säkerhetsåtgärder för IKT-produkter och IKT-tjänster.

3. År 2027 får Upphandlingsmyndigheten i samverkan med NCSC i uppdrag att analysera befintligt stöd gällande avtalsuppföljning och vid behov uppdatera stödet till offentliga organisationer och leverantörer för att de på ett strukturerat och effektivt sätt ska kunna genomför avtalsuppföljningar för IKT-produkter och IKT-tjänster. Uppdraget avslutas år 2028 varefter uppdateringsbehov sker inom ordinarie verksamhet.

4. Upphandlingsmyndigheten och NCSC har från 2027 ett uppdrag att i samverkan ta fram och förvalta cybersäkerhetskaven i nivåer samt erbjuda en kriterietjänst eller motsvarande. Arbetssätt för att identifiera, uppdatera och följa upp cybersäkerhetskrav, sammanställa dem i gemensamma skyddsnivåer samt utveckla instruktioner för hur cybersäkerhetkrav väljs och kompletteras utifrån organisationens specifika risker och behov tas också fram.

Indikatorer

Referenser

Hantering av sårbarheter och sårbarhetsinformation

Enligt NIS 2-direktivets artikel 7.2 c) Riktlinjer för hantering av sårbarheter, inbegripet främjande och underlättande av samordnad delgivning av information om sårbarheter enligt artikel 12.1.

Definitioner och begrepp

Det finns en rad specifika uttryck som används inom området samordnad delgivning av information om sårbarheter respektive sårbarhetshantering. Uttrycken härrör dels från internationella standarder, dels från reglering. Uttryck av central betydelse för denna policy utgår i första hand från definitioner i den svenska översättningen av NIS2-direktivet, i andra hand från den svenska översättningen av Cyberresiliensförordningen (CRA). Om definitioner av centrala uttryck inom samordnad delgivning av sårbarhetsinformation saknas i reglering, används en svensk översättning av definitionerna i NIS Cooperation Groups vägledning om implementering av nationella policyer för samordnad delgivning av sårbarhetsinformation[99]. Om definitioner av centrala uttryck saknas i den, används definitioner i etablerad internationell standard för samordnad delgivning av information.

Rapportör: En sårbarhetsforskare som identifierar och rapporterar en sårbarhet.[100]

Samordnad delgivning av information om sårbarheter: En strukturerad process genom vilken sårbarheter i programvara rapporteras till tillverkaren eller leverantören av berörd IKT-produkt eller IKT-tjänst. Detta för att göra det möjligt att analysera och åtgärda sårbarheten innan detaljerad information om sårbarheten meddelas tredjeparter eller allmänheten. Samordnad delgivning av information om sårbarheter bör även inbegripa samordning mellan den rapporterande fysiska eller juridiska personen och tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna vad gäller tidpunkten för åtgärdandet och offentliggörandet av sårbarheter. [101] På engelska kallas detta uttryck Coordinated Vulnerability Disclosure (CVD) och är det uttryck som används i denna policy.

Samordnare: Betrodd mellanhand som underlättar interaktionen mellan en fysisk eller juridisk person, som rapporterar en sårbarhet, och tillverkaren eller

[99] Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies, NIS Cooperation Group, 2023
[100] Översättning från NIS 2 CG vägledning - Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies, NIS Cooperation Group, 2023
[101] NIS 2-Direktivet skäl 58 (s12). https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32022L2555

leverantören av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna, på begäran av endera parten.

Sårbarhet: En svaghet, känslighet eller brist hos IKT-produkter eller IKT-tjänster som kan utnyttjas genom ett cyberhot.

Sårbarhetsforskare: Fysisk eller juridisk person, som avsiktligt eller oavsiktligt, och med gott uppsåt söker efter och utforskar potentiella sårbarheter. [102]

Tillverkare: En fysisk eller juridisk person som utvecklar eller tillverkar produkter med digitala element, eller som låter utforma, utveckla eller tillverka produkter med digitala element, och saluför dessa under eget namn eller varumärke, vare sig mot betalning eller kostnadsfritt.

Introduktion

Den här policyn gäller sårbarhetshantering i digitala miljöer och beskriver hur Sverige bör agera för att stärka processerna för samordnad delgivning av sårbarhetsinformation och hantering av sårbarheter i enskilda organisationer. Den syftar även till att stärka svenska organisationers möjligheter att ta del av sådan information och vidta nödvändiga sårbarhetsrättande åtgärder utifrån den.

Det är avgörande att allt fler aktörer i samhället stärker sina sårbarhetsrättade förmågor. Därtill behöver fler aktörer i samhället bidra och samverka i allt högre utsträckning inom det som kallas för samordnad delgivning av sårbarhetsinformation (CVD-processen). Det inkluderar de som upptäcker sårbarheter (s.k. sårbarhetsforskare), de som rapporterar sårbarheter, tillverkare och leverantörer av digitala produkter och tjänster som rättar och erbjuder säkerhetsuppdateringar för sårbarheter, användare av mjukvaror samt de aktörer som koordinerar och stöttar arbetet i processen.

Information om sårbarheter kan förmedlas direkt från tillverkaren till användarna eller så kan den som upptäckt sårbarheten rapportera sårbarhetsinformation till en betrodd förmedlare, som centralt koordinerar delgivningen av sårbarhetsinformation. Enligt NIS 2-direktivet ska den nationella CSIRT-enheten inneha rollen som samordnare och vara en betrodd förmedlare av sårbarhetsinformation.

Avgränsning

Avgränsning inte helt fastställd.

[102] Översättning från NIS 2 CG vägledning - Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies, NIS Cooperation Group, 2023

Nulägesbild

Sårbarheter i digitala tjänster och produkter upptäcks allt snabbare. Utnyttjandet av orättade sårbarheter är idag ett vanligt sätt för antagonistiska hotaktörer att få fotfäste i en it-miljö efter nätfiske (phishing).[1] Upptäckterna sker både manuellt och med automatiserade metoder - av hotaktörer, tillverkare, sårbarhetsforskare och enskilda personer med it-säkerhetsintresse. Nya metoder och tekniker för att utnyttja sårbarheter utvecklas kontinuerligt där artificiell intelligens används i allt större utsträckning för att både identifiera, utveckla och automatisera utnyttjandet av sårbarheter.[103] Därutöver finns en global marknad över försäljning av sårbarhetsinformation på en vit, grå respektive svart marknad. När det gäller den svarta, illegala marknaden sker den exempelvis via darkweb, specialiserade chattforum eller marknadsplatser.[104]

Utnyttjande av s.k. zero-day-sårbarheter, det vill säga sådana sårbarheter som ännu inte är kända hos tillverkaren, utnyttjas i allt högre utsträckning än tidigare av antagonistiska cyberhotaktörer, underrättelsemyndigheter samt brottsbekämpande organ.

Den snabba upptäckten av sårbarheter, liksom försäljningen av information av sårbarheter, föranleder behov av effektiv sårbarhetshantering i samhället – hos enskilda användande organisationer, hos tillverkare och koordinerare.

Standardisering och internationellt samarbete

En effektiv CVD-process är beroende av internationellt samarbete och standardisering. Det finns ett antal etablerade standarder för CVD, såsom ISO/IEC 29147:2018, där tillverkare kan hitta vägledning om hur de kan förbereda sig för att effektivt hantera och åtgärda sårbarheter som upptäcks eller rapporteras i deras produkter. Internationellt finns vidare ett antal vedertagna arbetssätt och tjänster för informationsdelning, liksom klassificering, av upptäckta sårbarheter. Den amerikanska organisationen MITRE ansvarar för att organisera och utveckla MITRE CVE, en öppet tillgänglig och standardiserad katalog över sårbarheter.[105] Varje sårbarhet tilldelas en unik identifierare, ett så kallat CVE-ID, och systemet har sedan flera år tillbaka fungerat som branschstandard. Så kallade CVE Numbering Authorities (CNA) kan tilldela CVE-ID. CNA:erna kan vara mjukvarutillverkare, tjänsteleverantörer eller CERT-verksamheter. Det innebär att information om sårbarheter kan delas på ett strukturerat sätt i olika sårbarhetsdatabaser.

[103] ENISA Threat Landscape 2025, https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025_0.pdf
[104] OECD Encouraging vulnerability treatment, 2021, https://www.oecd.org/en/publications/encouraging-vulnerability-treatment_0e2615ba-en.html
[105] Lanserat av MITRE Corporation 1999, https://cybercompliancewatch.org/mitre-cve/

Den europeiska cybersäkerhetsbyrån Enisa, OECD och NIS Cooperation Working Group har även publicerat vägledningar och riktlinjer på området.

I syfte att öka stabiliteten och minska beroendet till utomeuropeiska aktörer har EU, genom Enisa, lanserat en egen sårbarhetsdatabas (EUVD) i maj 2025. Denna databas motsvarar den amerikanska nationella sårbarhetsdatabasen National Vulnerability Database (NVD)[106] som National Institute of Standards and Technology (NIST) tillhandahåller. Enisa har i samband med detta även registrerats som en s.k. CVE Numbering Authority (CNA), som innebär att sårbarheter rapporterade till EU:s CSIRT-enheter kan tilldelas CVE-ID i det internationella ekosystemet för sårbarhetsinformation. För att ytterligare stärka Enisas roll och möjligheter på området är Enisa sedan november 2025 en s.k. Root i CVE-programmet.[107] Genom denna roll blir Enisa en central kontaktpunkt inom CVE-programmet för nationella myndigheter inom EU, medlemmar inom EU CSIRT-nätverket och för Enisas samarbetspartners.

I Sverige finns enstaka forum och mötesplatser för informationsgivning, erfarenhetsutbyte och kompetensutveckling om sårbarheter och sårbarhetsrättning samt reglering på området. Nordic Software Security Summit[108] och SEC-T[109] finns. CERT-SE deltar även i CVD-relaterade diskussioner i EU:s nätverk för nationella CSIRT-enheter.

Samordnad delgivning av sårbarhetsinformation liksom rapportering av sårbarheter regleras

CVD-processen har tidigare varit oreglerad. Detta förändras i och med EU:s regelverkspaket för cyberområdet, med reglering såsom NIS 2-direktivet (som i Sverige implementeras genom Cybersäkerhetslagen, CSL), Cyberresiliensförordningen (CRA) och Cybersäkerhetsakten (CSA).[110] Sammantaget fastställer och tydliggör dessa regelverk hur CVD-processer ska genomföras inom EU:s medlemsstater samt hur samordningen mellan dem ska ske.

CRA reglerar tillverkares ansvar för säkerheten i digitala produkter under produktens hela livscykel. Den ställer krav på tillverkarnas processer för identifiering, dokumentation, hantering och delgivning av information om sårbarheter i deras produkter. Den introducerar även krav på att sårbarheter ska

[106] https://digital-strategy.ec.europa.eu/en/news/eu-launches-european-vulnerability-database-boost-its-digital-security
[107] https://www.enisa.europa.eu/news/stepping-up-our-role-in-vulnerability-management-enisa-becomes-cve-root
[108] https://nsss.se/
[109] https://sec-t.org/
[110] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten)

rapporteras till den nationella CSIRT-enheten, varav aktivt utnyttjade sådana ska rapporteras inom 24 timmar.

Kraven i CRA införs stegvis under 2024 till 2027. I september 2026 börjar bestämmelserna om rapportering att gälla. I artikel 15 beskrivs frivillig rapportering av bl.a. sårbarheter till den nationella koordinerande CSIRT-enheten, vilket kan tydliggöra vart sårbarhetsforskare (t.ex. upptäckare, etiska hackare, penetrationstestare) kan vända sig avseende identifierade sårbarheter i produkter som tillgängliggörs i EU.

CSL ställer bland annat krav på säkerhet vid underhåll av nätverks- och informationssystem, innebärande identifiering, hantering och informationsgivning om sårbarheter. Dessutom finns krav på sårbarhetsrapportering och hantering av sårbarheter inom ramen för cybersäkerhetscertifiering i enlighet med CSA.

Den nationella samordnarrollen av sårbarhetsinformation regleras genom NIS 2-direktivet och CRA. Samordnarrollen är en delroll som ingår i rollen som nationell CSIRT-enhet. Rollen bygger på etablerad internationell praxis med ursprung i ramverk från CERT/CC, FIRST och ISO/IEC 29147. Roller och begrepp skiljer sig dock mellan de olika EU-regleringarna.

Den nationella CSIRT-enhetens roll och förmåga som betrodd samordnare av sårbarhetsinformation

Den nationella CSIRT-enheten innehar rollen som betrodd samordnare inom CVD-processen. Myndigheten för civilt försvar har varit utsedd till Sveriges CSIRT-enhet sedan 2018. Myndigheten har i huvudsak utfört rollen inom ramen för CERT-SE.[111] I artikel 12 NIS 2-direktivet kravställs den nationella CSIRT-enhetens uppgifter till bland annat att:

- ta emot sårbarhetsrapporter från sårbarhetsforskare och rapportörer samt att stödja dessa roller,
- underlätta interaktionen mellan en rapportör, eller sårbarhetsforskare, och tillverkaren, eller leverantören, av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna på begäran av endera parten,
- identifiera och kontakta berörda parter,
- agera som en betrodd mellanhand, samt förhandla tidsramar för delgivning av information samt samordna arbetet.[112]

[111] Enligt Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster

[112] Art.12 EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet)

Myndigheten för civilt försvar, CERT-SE, förbereder verksamheten på att leva upp till kraven på nationell CSIRT-enhet i enlighet med NIS 2-direktivet. Det innebär bl.a. att verksamheten förbereder för att ta emot fler sårbarhetsärenden och att teknisk infrastruktur för sårbarhetsrapportering ska anslutas till det gemensamma europeiska systemet.

Regeringens beslut den 20 november 2025 om att samla cybersäkerhetsverksamhet hos Nationellt cybersäkerhetscenter, NCSC/FRA medför att Försvarets radioanstalt (FRA) blir huvudansvarig för den nationella CSIRT-enheten, gemensam kontaktpunkt och cyberkrishanteringsmyndighet. Myndigheten för civilt försvar och FRA förbereder för att kunna utföra CSIRT-enhetens uppgifter även hos FRA inom ramen för NCSC.

CERT-SE informerar sedan flera år om aktuella sårbarheter genom bl.a. veckobrev och s.k. blixtmeddelanden när kritiska sårbarheter finns att informera om samt hantera.

Incitament för sårbarhetsrapportering i nuläget

Ytterligare en typ av samordnare av sårbarhetsinformation är s.k. Bug Bounty-plattformar som erbjuder upptäckare av sårbarheter att rapportera in sådana till sig, och sedan vidarebefordrar dem till anslutna tillverkare. I vissa fall utgår en ekonomisk ersättning till upptäckaren. Bug Bounty-plattformar kan ses som ett komplement till den nationella samordnarens roll och som ett sätt att uppmuntra fristående sårbarhetsforskare att rapportera sårbarheter. Internationellt drivs Bug Bounty-program både av privata och statliga aktörer. Ett exempel är The Sovereign Tech Resilience program som finns i Tyskland.[113]

Legala förutsättningar för sårbarhetsforskare saknas i nuläget

Den som gör sig skyldig till dataintrång, dvs. olovligen tränger sig in i ett it-system där data blir behandlad, lagrad eller överförd elektroniskt kan enligt 4 kap. 9 c brottsbalken (1962:700) bli dömd med böter och fängelse. Det finns dock situationer när aktiviteter som tangerar dataintrång genomförs med gott uppsåt att hitta säkerhetsbrister.

Trots genomförandena av CRA, CSL och CSA, saknas ett legalt skydd för sårbarhetsforskare, som inte har ägarens tillstånd att leta efter sårbarheter i programvaror eller system. Av skäl 57 Cyberresiliensförordningen framgår det följande. *Medlemsstaterna bör sträva efter att i största möjliga utsträckning ta itu med de utmaningar som sårbarhetsforskare ställs inför, inbegripet deras potentiella utsatthet för straffrättsligt ansvar, i enlighet med nationell rätt. Med tanke på att fysiska och juridiska personer som forskar om sårbarheter skulle kunna riskera straff- och civilrättsligt ansvar i vissa*

[113] https://www.sovereign.tech/programs/bug-resilience

medlemsstater uppmuntras medlemsstaterna att anta riktlinjer för icke-lagföring av forskare inom informationssäkerhet och befrielse från civilrättsligt ansvar för deras verksamhet.

Sårbarhetsforskare kan mötas av rättsliga repressalier, t.ex. genom åtal eller stämning från tillverkare och leverantörer av programvaran som innehar sårbarheten. Det kan även innebära regelöverträdelser inom dataskyddsområdet (GDPR), immaterialrätten (t.ex. åtkomst till kod) samt bryta mot användarvillkor. NIS Cooperation Groups *Guidelines on implementing national coordiniated vulnerability disclosure policies* uppmuntrar medlemsstater att vidta åtgärder för att stärka det legala skyddsnätet för sårbarhetsforskare.[114]

Offentlighets- och sekretesslagen (2009:400) kan komma att kompletteras med nya sekretessregler för att säkerställa konfidentialitet vid inrapportering av sårbarheter till myndigheter.

Låg kännedom om CVD-process och varför den är viktig för samhället

Trots att etablerade standarder och ramverk finns sedan flera år indikerar inkomna frågor och det låga antalet inrapporterade sårbarhetsärenden till den nationella CSIRT-enheten att många organisationer har låg kännedom om processen och varför det är viktigt att de deltar i den. Tillverkare, leverantörer och distributörer av programvara och hårdvara, liksom användare av programvara bedöms generellt ha låg kännedom om samordnad delgivning av sårbarhetsinformation. Det finns dock vissa mogna tillverkare, sårbarhetsforskare och särskilt it-intresserade med god kännedom om processen. Utbildning inom etisk hackning erbjuds på bland annat ett antal universitet och högskolor i Sverige. Den nationella CSIRT-enheten avser publicera information om samordnad delgivning av sårbarhetsinformation på sin webbplats.

Bristfällig sårbarhetshantering hos enskilda organisationer

Organisationer förlitar sig idag på en stor mängd programvaror och system för att kunna bedriva egen verksamhet samt för att erbjuda tjänster och produkter. Mängden och variationen av programvaror och system som kräver förvaltning ökar över tid. I vissa fall förvaltar organisationen programvaror och system i egen regi. I andra fall har organisationer lagt ut system, programvaror och tjänster hos en extern part. Oaktat vem som sköter programvaruhantering krävs, att organisationer genomför, eller ställer krav på, ändamålsenlig sårbarhetshantering samt förvaltar, eller ställer krav på, förvaltning av de programvaror som nyttjas.

[114] Guidelines on implementing national Coordinated Vulnerability Disclosure (CVD) policies, kapitel 3, s.5, https://ec.europa.eu/newsroom/dae/redirection/document/99973

Dessutom består ofta system och tjänster av kod och mjukvarukomponenter från olika tillverkare eller utvecklingsprojekt. Organisationer saknar ofta en tydlig överblick över vilka system och tjänster som påverkas i händelse av en upptäckt sårbarhet. CRA kommer från och med december 2027 att ställa krav på mjukvarutillverkare att kunna producera denna typ av mjukvaruförteckningar, så kallade Software Bill of Material (SBOM).

Det finns ett antal ytterligare utmaningar som påverkar enskilda organisationers förmåga att hantera sårbarheter på ett adekvat sätt:

- Bristande kunskap om behovet av att genomföra säkerhetsuppdateringar och att agera på information från CSIRT-enheten skyndsamt samt att sårbarhetsrättningar kan medföra nya sårbarheter som t.ex. skadlig kod.
- Otydliga eller icke-ändamålsenliga organisationsstrukturer, mandat och arbetssätt för att hantera sårbarheter på ett effektivt sätt.
- Bristfälliga tekniska system samt processer för sårbarhetshantering. Dels när det gäller kännedom om organisationens nyttjade programvaror och programvaruversioner. Dels när det gäller prioritering och hantering av sårbarheter på ett ändamålsenligt sätt.[115]
- Avsaknad av tillräckliga ekonomiska och personella resurser för att för genomföra säkerhetsuppdateringar eller för vidtagande av andra nödvändiga säkerhetsåtgärder.
- Att sårbarhetsinformation inte når fram till den berörda organisationen.

Det finns flera etablerade modeller och ramverk för sårbarhetshantering som verksamheter kan tillämpa, men de behöver anpassas till verksamhetens förutsättningar och risknivå.

Nya föreskrifter om säkerhetsåtgärder enligt CSL innehåller bl.a. krav på hantering av sårbarheter och säker livscykelhantering för verksamhetsutövare som omfattas av CSL. Vidare ställer EU:s regleringar, Cybersäkerhetsförordningen och CRA, krav på inbyggd säkerhet och säker livscykelhantering i programvaror.

Analys av nuläget

Låg kännedom om samordnad delgivning av information om sårbarheter i samhället

Det är positivt att det finns internationell branschpraxis, ISO-standarder och stödmaterial för samtliga roller inom CVD-processen. Det är dessutom positivt att utbildning inom etisk hackning erbjuds i Sverige samt att information och råd från den nationella CSIRT-enheten finns, vilket ökar kännedomen om CVD. Däremot är det negativt att det råder en låg kännedom om CVD-processen och att få

sårbarheter rapporteras till tillverkare, CSIRT-enheter eller annan samordnare. Samtidigt är det positivt att ny EU-reglering, såsom CRA, införs, vilken syftar till att ändra på detta.

Det är också negativt att EU-regleringarnas begrepp inte stämmer överens med de begrepp som används i standarder på området, vilket kan skapa problem för organisationer att tolka vad de behöver göra. Det kan även leda till dubbelarbete för organisationer som har etablerade processer enligt vedertagen standard, men som måste säkerställa att dessa är i linje med EU-regleringens definitioner.

Nationellt och internationellt samarbete

Det är bra att ett grundläggande nationellt och internationellt samarbete förekommer och att Europa med exempelvis Enisa prioriterar sårbarhetsfrågor och har lanserat EUVD, men det är samtidigt negativt att potentialen i sådana samarbeten inte nyttjas mer. Ett bättre utvecklat samarbete kan bidra till snabbare informationsdelning, bättre samordning mellan berörda aktörer och effektivare åtgärder, vilket i sin tur kan minska risken för att kända sårbarheter utnyttjas innan de har hanterats. Att dessa möjligheter går förbi beror på att de oftast inte är kända för dem som skulle kunna engagera sig i dem, samt att det finns få aktörer på området.

Rättsliga förutsättningar för samordnad delgivning, sårbarhetshantering förbättras

Det är positivt att samordnad delgivning av information om sårbarheter regleras i EU samt i Sverige genom CRA, CSL och Cybersäkerhetsakten (CSA) och samt att nya sekretessregler om anonyma rapportörer och inrapporterad information kan komma i OSL. CRA uppställer omfattande cybersäkerhetskrav i produkter med digitala element.[116] Informationsgivning och tillsyn från tillsynsmyndigheter och marknadskontrollmyndigheter kommer sätta ljus på reglerna samt förbättra regelefterlevnaden när det gäller bl.a. rapportering av sårbarheter och framtagning av programvarurättningar, vilket är gynnsamt.

Avsaknaden av tydliga legala rättigheter för att bedriva sårbarhetsforskning är problematisk, eftersom den kan leda till att både nya sårbarheter och förekomster av redan kända sårbarheter inte upptäcks i den omfattning som samhället behöver. Sårbarhetsforskare med vilja och kompetens att undersöka mjukvara och internetexponerade system i syfte att ansvarsfullt rapportera sårbarheter innan de utnyttjas av hotaktörer riskerar exempelvis att åtalas för dataintrång. Detta medför att sårbarhetsforskare avstår från verksamhet som annars hade kunnat vara till stor nytta för såväl organisationer som samhället i stort

[116] Bilaga I, Väsentliga cybersäkerhetskrav CRA

Hantering av sårbarheter i den egna verksamheten

Det är positivt att CSL och tillhörande föreskrifter ställer krav på säker livscykelhantering, programvarusäkerhet och sårbarhetshantering. Något som väntas leda till att verksamhetsutövare som omfattas av CSL förbättrar sitt arbete med sårbarhetshantering. Det är också positivt att CRA och EU:s cybersäkerhetsakt förväntas driva utvecklingen mot ökad inbyggd säkerhet i programvaror hos mjukvarutillverkare, leverantörer och distributörer av programvaror. Därtill är det positivt att cybersäkerhetscertifiering inom ramen för EU:s cybersäkerhetsakt (2019/881) ställer krav på sårbarhetshantering och rapportering av sårbarheter.

Det är problematiskt att många organisationer i nuläget inte avsätter tillräckligt med ekonomiska och personella resurser till arbetet med att identifiera, prioritera och åtgärda sårbarheter. Detta leder till att sårbarhetshanteringen inte blir ändamålsenlig, vilket kan leda till en ökad risk och exponering för incidenter med potentiellt stora konsekvenser. Resursbristen påverkar även förmågor om att upprätta, förvalta och tillämpa nödvändiga rutiner. Det kan finnas flera orsaker till att organisationer inte avsätter tillräckliga resurser. Exempelvis att organisationen inte känner till, eller har bedömt, vilka faktiska ekonomiska, affärs- och konkurrensmässiga, samhällsviktiga eller förtroende- och integritetsmässiga konsekvenser incidenter kan medföra.

Det är även negativt att många organisationer har en låg grad av kännedom om sina installerade programvaror, programvaruversioner och programvaruberoenden. Detta försvårar möjligheten att identifiera vilka system som kan påverkas när nya sårbarheter offentliggörs och bedöma vilka system och programvaror som behöver prioriteras när det gäller att utföra säkerhetsuppdateringar eller behov av vidtagande av andra åtgärder. Det kan finnas flera orsaker till detta, exempelvis att organisationen inte har kunskap om varför det är viktigt att ha en samlad och uppdaterad bild över samtliga sina programvaror och programvaruversioner, att organisationen inte har haft resurser för att införskaffa och använda ändamålsenliga system och processer för att kunna säkerställa en god överblick över detta.

Att ansvarsfördelningen för genomförande av säkerhetsuppdateringar av programvaror är icke-ändamålsenlig är vidare en utmaning. En orsak till detta kan vara att ledningen inte avsätter tillräckligt med tid för styrning, prioritering och uppföljning av det systematiska säkerhetsarbetet. Effekterna blir således att säkerhetsuppdateringar ibland genomförs för sent eller på ett inkonsekvent sätt, vilket innebär att kända sårbarheter i verksamhetens nyttjade programvaror finns kvar längre än nödvändigt.

Det är därtill negativt att många organisationer saknar eller inte använder ändamålsenliga och dokumenterade processer för prioritering samt hantering av

sårbarheter. Det medför att beslut om genomförande av säkerhetsuppdateringar tas ad hoc eller utan ett helhetsperspektiv som beaktar organisationens system och programvaror, vilket sedan kan utnyttjas av hotaktörer. Ett sådant arbetssätt medför att hanteringen av sårbarheter inte sker systematiskt och att system kan lämnas oskyddade längre än nödvändigt. Det kan finnas flera orsaker till bristfälliga processer för sårbarhetshantering. En är att organisationer inte har haft tillräckligt med resurser för att identifiera eller saknar kunskap om ändamålsenliga processer på området.

Det är positivt att CERT-SE löpande informerar om aktuella sårbarheter via veckobrev och blixtmeddelanden, men det är negativt att det saknas information om hur sårbarhetsinformation tas emot och vilka faktiska åtgärder informationen leder till. En bristande förståelse för budskapet riskerar att fördröja eller helt förhindra nödvändiga uppdateringar.

Målbild 2029

Samordnad delgivning av information om sårbarheter har ett högt deltagande och CVD är ett etablerat och väl förstått begrepp

Tillverkare, sårbarhetsforskare, verksamhetsutövare enligt Cybersäkerhetslagen och den nationella CSIRT-enheten har en gemensam förståelse för innebörden av begrepp och processer inom CVD. Dessa deltar även aktivt i CVD-processen genom att ta emot sårbarhetsinformation, rätta sårbarheter och informera om sårbarheter på ett ansvarsfullt sätt i relation till risker för organisationer som använder mjukvaran och för samhället i stort.

Över 50 procent av tillverkare, samtliga statliga myndigheter och minst 80 procent av övriga offentliga aktörer[117] har publicerade CVD-policys, security.txt och tillräckligt säkra rapporteringskanaler. Detta i syfte för att underlätta och uppmuntra till ansvarsfull rapportering av upptäckta sårbarheter direkt till berörd tillverkare eller annan ansvarig organisation för sårbarhetshantering.

Den nationella CSIRT-enheten är en betrodd nationell samordnare av sårbarhetsinformation

Den nationella CSIRT-enhetens roll som samordnare av delgivning av sårbarhetsinformation är känd bland alla verksamhetsutövare enligt Cybersäkerhetslagen, tillverkare respektive distributörer av produkter med digitala element enligt Cyberresiliensförordningen samt sårbarhetsforskare.

[117] 290 kommuner, 21 regioner

Den nationella CSIRT-enheten i sin roll som samordnare av delgivning av sårbarhetsinformation är betrodd, vilket gör att även frivillig rapportering av sårbarheter sker i hög utsträckning till den nationella samordnaren. Minst 25 procent av tillverkare rapporterar frivilligt sårbarheter i enlighet med CRA i slutet av 2029.

Den nationella CSIRT-enheten är en effektiv nationell samordnare av sårbarhetsinformation

Den nationella CSIRT-enheten har en fullt utbyggd CVD-funktion och har tekniska system som är integrerade med relevanta europeiska plattformar för sårbarhetsinformation.

Det finns ett väl utvecklat koordinerande arbete mellan nationell samordnare, tillverkare och organisationer för att gemensamt hantera situationer där sårbarheter har inverkan på många aktörer. Dessa tar också del av den nationella samordnarens informationsutskick om upptäckta sårbarheter och agerar på denna information. Den nationella samordnaren följer också upp att mottagare agerar på informationen. År 2029 utgör CSL, kompletterande bestämmelser i OSL samt andra relevanta regleringar ett sammanhängande och praktiskt fungerande regelverk för sårbarhetshantering.

Organisationers rättning av sårbarheter

Majoriteten av organisationer inom både offentlig och privat sektor i Sverige innehar och tillämpar ändamålsenliga processer för sårbarhetshantering. Det innebär att de identifierar, prioriterar, åtgärdar och informerar om sårbarheter på ett ändamålsenligt sätt och att de installerar säkerhetsuppdateringar inom skälig tid efter att en sårbarhet uppdagats.

Organisationer har tillgång till tydliga programvaruförteckningar från leverantörer (SBOM) och s.k. asset management-system som ger en bild över vilka sårbarheter som utgör en risk för deras verksamhet. För organisationer med samhällsviktiga funktioner sker detta inom tydligt fastställda tidsramar. Incidenter där kända, men orättade sårbarheter, utnyttjas har minskat betydligt.

Minst 90 procent av de som deltar i Cybersäkerhetskollen uppger att de har definierade processer för sårbarhetsrättande ändringshantering. Minst 80 procent uppger också att de har inventerat sina installerade programvaror som även innefattar programvaruförteckningar (SBOM).

Rättsliga förutsättningar

Sårbarhetsforskare kan agera inom tydliga rättsliga ramar, där ansvarfullt agerande skyddas och uppmuntras. Rollen som sårbarhetsforskare (upptäckare) och rapportör är tydlig, legitim och meningsfull. Den är dessutom tydligt legalt

avgränsad, för att specifikt skydda rollens etiska ansvarsområde. Rättsligt skydd för säkerhetsforskare att aktivt leta efter och rapportera in sårbarheteter utifrån givna etiska ramar, ett så kallat Safe Harbour-ramverk har införts.

Internationellt samarbete

Sverige deltar aktivt i och utvecklar internationella samarbeten samt arbetar för standardisering. Sverige deltar också aktivt i internationella samarbeten för att förebygga brottslig verksamhet. Till exempel att motverka illegal handel med sårbarheter.

Åtgärder för att uppnå målbilden

Förbättra kännedomen och öka deltagandet i processen för samordnad delgivning av information om sårbarheter (CVD)

Den nationella CSIRT-enheten ska utforma och publicera målgruppsanpassade vägledningar och mallar för CVD-policys och processer 2027. Vägledning ska tas fram till tillverkare, enskilda organisationer som använder mjukvara respektive till verksamheter som har offentligt exponerade system/webbsidor.

Under 2028 ska den nationella CSIRT-enheten ta fram och publicera utbildningsmaterial om CVD i form av nano-learning till relevanta målgrupper.

Fler tillverkare är CVE Numbering Authorities

För att antalet inkomna sårbarhetsärenden via CVD till tillverkare och den nationella samordnaren ska öka ska fler tillverkare uppmuntras till att bli CVE Numbering Authorities (CNA), vilket ska underlättas genom att den nationella CSIRT-enheten under 2028 tar fram vägledning för hur tillverkare ansöker om att bli samt vilka krav som ställs på CNA.

Inkludera CVD-processen i produktcertifieringar

För att uppmuntra till att tillverkare av mjukvara arbetar aktivt med CVD ska lämplig ansvarig myndighet säkerställa att de certifieringar som erbjuds innehåller krav på CVD-processer.

Säkerställa förtroendet för den nationella CSIRT-enheten som den nationella samordnaren av sårbarhetsinformation

Nationell lägesbild över sårbarheter

Under 2027 etablerar NCSC format och processer för att kunna tillhandahålla en nationell lägesbild över sårbarheter och sårbarhetsexploatering inklusive

rekommendationer relaterade till sårbarhetshantering. Lägesbilden är målgruppsanpassad. Detta kan även ske inom ramen för andra årsrapporter som NCSC publicerar.

Vidareutveckla en effektiv nationell CSIRT-enhet

Införande av effektiva systemstöd och integration med EU-entiteter

Den nationella CSIRT-enheten deltar i utvecklingen av gemensamma arbetssätt och teknikstöd internationellt för att effektivt kunna hantera sårbarhetsärenden i såväl en svensk som europeisk kontext.

Uppföljning av informationsinsatser om aktuella sårbarheter

Under 2026 tar CSIRT-enheten fram modeller för uppföljning av de informationsutskick om sårbarheter som enheten genomför i syfte att kunna mäta hur stor del av den information som skickas ut som leder till åtgärder av enskilda organisationer.

Förstärka organisationers sårbarhetshantering

För att säkerställa att organisationer som använder it- och ot-system innehar och tillämpar fungerande och väldefinierade processer för sårbarhetshantering krävs ett antal åtgärder.

Stöd och rådgivning

NCSC och den nationella CSIRT-enheten tar under 2026 fram vägledning om sårbarhetshantering och sårbarhetsrättning riktad till enskilda organisationer. Från och med 2027 ska Cybersäkerhetsrådgivningen tillsammans med den nationella CSIRT-enheten erbjuda rådgivning avseende sårbarhetshantering.

Under 2027 ska NCSC tillsammans med lämplig ansvarig myndighet ta fram vägledning om kravställning gällande sårbarhetshantering och samordnad delgivning av sårbarhetsinformation vid upphandling av IKT-tjänster och IKT-produkter (t.ex. tillhandahållande av SBOM, överenskomna tidsfrister för information om upptäckt av sårbarhetsinformation och tidsfrister för tillhandahållande av sårbarhetsrättande uppdatering).

Från och med 2027 ska Cybersäkerhetskollen kompletteras med specifika frågor rörande organisationernas arbete med sårbarhetshantering och sårbarhetsrättning.

Förbättrade rättsliga förutsättningar för sårbarhetsforskning ska komma på plats i nationell reglering

För att skapa ett bättre legalt ramverk för sårbarhetsforskare ska möjliga lagstiftningsförändringdringar för att införa ett Safe Harbour-ramverk för sårbarhetsforskare utredas under 2027.

CSIRT-enheten ska bidra aktivt i det internationella samarbetet

För att stärka Sveriges deltagande i det internationella samarbetet ska den nationella CSIRT-enheten etablera sig som CNA i CVE-programmet under 2028. På sikt ska den nationella CSIRT-enheten även vidta åtgärder för att kunna bli Top Level CNA och på så sätt ha möjlighet att registrera svenska organisationer som vill bli CNA.

Indikatorer

Referenser

Det öppna internets offentliga kärna

Enligt NIS 2-direktivets artikel 7.2 d) Riktlinjer för att upprätthålla den allmänna tillgängligheten, integriteten och konfidentialiteten hos den offentliga kärnan i det öppna internet, inbegripet, i tillämpliga fall, cybersäkerheten hos undervattenskablar.

Definitioner och begrepp

Den offentliga kärnan består av internets nyckelprotokoll och fysiska infrastruktur som underbygger internets grundläggande funktionalitet. Den fysiska infrastrukturen innefattar nationella stamnät och noder, undervattenskablar med tillhörande infrastruktur, samt satellitkommunikation i den omfattning som den fyller motsvarande funktion som nämnd kabelinfrastruktur.

Introduktion

Internet är byggt för robusthet och motståndskraft. Den decentraliserade infrastrukturen, i kombination med standardiserade protokoll, gör det möjligt för internet att fortsätta fungera även om delar av nätverket fallerar.

Det kan samtidigt konstateras att internet inte är felsäkert. Allvarliga avbrott i den offentliga kärnan kan till följd av systemfel, misstag, sabotage eller cyberangrepp, få omfattande konsekvenser för samhället och nationell säkerhet. Det öppna internets offentliga kärna utgör således en viktig samhällsfunktion.

Internet och dess offentliga kärna utgörs av en global infrastruktur som saknar ett enhetligt ägarskap. Det utvecklas, drivs och underhålls av ett stort antal oberoende aktörer, från internationella standardiseringsorgan och internetoperatörer, till privata företag och ideella organisationer. Dess offentliga kärna omfattar de gemensamma och gränsöverskridande infrastrukturer, protokoll och system som möjliggör ett öppet, sammanhängande och tillgängligt internet för alla användare i Sverige.

Avgränsning

Avgränsning inte helt fastställd.

Nulägesbild

I Sverige hanteras den offentliga kärnan av internet av ett antal aktörer, både privata och offentliga. Nulägesbilden presenterar den offentliga kärnans beståndsdelar, aktörerna som upprätthåller dem och samverkansformer.

Den nya cybersäkerhetslagen trädde i kraft den 15 januari 2026. Lagstiftningen innebär att verksamheter som är viktiga för det öppna internets offentliga kärna kommer att behöva vidta ytterligare säkerhetsåtgärder, rapportera betydande incidenter och informera mottagare av deras tjänster om sådana och cyberhot som kan påverka dem.

Tillsynsmyndigheterna tar fram föreskrifter om säkerhetsåtgärder, skyldigheten att föra register om domännamn, vad som utgör en betydande incident samt om informations-skyldigheten vid betydande incidenter och betydande cyberhot. Tillsynsmyndigheterna utövar även tillsyn över verksamhetsutövare som har anmält sig för att säkerställa säkerhetsregleringens efterlevnad. Tillsynsmyndigheterna vägleder även om incidentrapportering och säkerhetsåtgärder.

Ansvarsprincipen gäller i Sverige, vilket innebär att den som ansvarar för en verksamhet under normala förhållanden också gör det i händelse av kris, höjd beredskap och krig. På nationell nivå ansvarar Post- och telestyrelsen för koordinering vid allvarliga samhällsstörningar. Nationella telesamverkansgruppen (NTSG) är viktig för samverkan mellan myndigheter och företag inom telekomsektorn. Verksamheten är lagreglerad och utpekade företag och myndigheter är skyldiga att delta i samverkan inom NTSG.

Nationella nät och noder

De nationella näten för fiberoptisk bredbandskommunikation – även kallade stamnät eller backbone-nät – kännetecknas av hög kapacitet och sammanlänkar Sveriges regionala bredbandsnät via knutpunkter. Knutpunkterna är centrala för de nationella nätens funktionalitet och tillgängligheten i den offentliga kärnan. De nationella näten är vidare anslutna till internationella nät genom bland annat undervattenskabel-infrastrukturen. Näten ägs av de stora nätoperatörerna samt av regionala och lokala stadsnätsoperatörer[118] i Sverige.

Undervattenskablar

Undervattenskablar utgör stommen i det globala internet och transporterar åtminstone 95 procent av världens datatrafik.[119] Undervattenskablarna ägs av privata företag som ansvarar för drift, underhåll och reparationer. Det finns ett svenskt fartyg som kan lägga och reparera undervattenskablar.[120]

[118] Det finns cirka 170 stadsnät i Sverige, varav 90 procent är kommunala. Stadsnäten är verksamma i 200 av landets kommuner och sammantaget äger de cirka 50 procent av all bredbandsinfrastrukturen, https://stadsnatsforeningen.se/stadsnatsfakta/
[119] Se exempelvis Enisas *rapport Undersea Cables – What is at stake?*
[120] https://www.sjofartstidningen.se/branschen-ett-fartyg-racker-inte/

EU tillkännagav i början av 2025 en handlingsplan med åtgärder för att stärka el- och telekominfrastruktur under vatten. I den ingår ett initiativ att bygga upp och stärka regionala nav för övervakning av undervattenskablar, vilket syftar till att främja situationsmedvetenhet och detekteringsförmåga.[121] Regeringen gav under 2025 bland annat MSB, PTS och Kustbevakningen uppdraget att gemensamt vidta åtgärder för att stärka förmågan att upptäcka och rapportera incidenter och störningar på undervattensinfrastruktur. Uppdraget är slutredovisat till regeringskansliet.[122]

I november 2025 beviljades fyra svenska aktörer 18 miljoner euro från Fonden för ett sammanlänkat Europa (FSE Digital) i syfte att förstärka den digitala undervattensinfrastrukturen.[123]

Inom ramen för Nato finns initiativet *Baltic Sentry* som, genom ökad militär närvaro i Östersjön, syftar till att bättre kunna skydda kritisk undervattensinfrastruktur. Kustbevakningen utgör operativ kontaktpunkt mot Nato-nätverket *Critical Undersea Infrastructure Network* (CUIN). Nätverket för samman bland annat militära aktörer, civila myndigheter och industripartners i syfte att stärka informationsspridning och samarbetet kring kritisk undervattensinfrastruktur. Kustbevakningens uppdrag genomförs i nära samarbete med Försvarsmakten och samverkan sker med andra myndigheter och privat sektor. Nato har även centret *Maritime Centre for Security of Critical Undersea Infrastructure* som koordinerar insatser mellan Natoallierade, partners och privat sektor. Sverige har tillsammans med andra länder i Östersjöregionen uttryckt vikten av ökat samarbete kring undervattensinfrastrukturen.[124]

Satellitkommunikation

Sverige är för satellitbaserad internetkommunikation i hög grad beroende av utländska kommersiella tjänster såsom Starlink, Eutelsat och SkyDSL, vilka primärt är anpassade för civila behov. Det finns tre markstationer på svenskt territorium som kan ta emot IP-baserad trafik.

På EU-nivå pågår projektet för satellitkommunikation *Infrastructure for Resilience, Interconnectivity and Security by Satellite* (IRIS²). IRIS² ska tillhandahålla kommunikationstjänster till EU och dess medlemsstater, privata företag och organisationer, samt EU-medborgare. Det kommer vara anpassat för militära och statliga ändamål (t.ex. säker kommunikation mellan ambassader) och kunna nyttjas vid krishantering och territoriell övervakning. IRIS² implementerar EuroQCI och

[121] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025JC0009
[122] *Redovisning av uppdraget att stärka det civila försvarets förmågeutveckling för att hantera incidenter kopplade till undervattensinfrastruktur*, Fö2025/00713.
[123] https://www.regeringen.se/pressmeddelanden/2025/11/18-miljoner-euro-till-sjokablar-starkt-reparationsformaga-och-kvantkommunikation/
[124] *Joint statement, Nordic and Baltic Ministers of Digitalisation*, publicerat den 20 november 2024 på regeringens hemsida.

kommer således nyttja avancerad krypteringsteknologi, inklusive kvantkryptografi, samt ha en secure-by-design-arkitektur för att säkerställa konfidentialiteten i dataöverföringen. IRIS² planeras vara i drift 2030.[125]

Border Gateway Protocol (BGP)

Ett centralt protokoll för att dirigera internettrafik mellan, samt inom, olika nät på internet är *Border Gateway Protocol* (BGP). BGP är sårbart för en typ av angrepp där hotaktören manipulerar rutterna och därmed kan omdirigera eller kapa trafik. För att komma till rätta med dessa problem har säkrare lösningar tagits fram. För BGP-protokollet finns certifikatinfrastrukturen *Resource Public Key Infrastructure* (RPKI). Enligt statistik från RIPE NCC 2024 hade RPKI implementerats i Sverige till drygt 70 procent (vilket var något lägre än många andra europeiska länder).[126] PTS genomförde under 2021 en BGP-tillsyn av de största svenska operatörerna som resulterade i att RPKI infördes av samtliga.

Domännamnsystemet (DNS)

DNS översätter domännamn till IP-adresser. I Sverige sköts och förvaltas en av världens totalt 13 rotnamnservertjänster (I-roten[127]).

Domain Name System Security Extensions (DNSSEC) är en säkerhetslösning som validerar att ett DNS-svar kommer från en legitim källa och inte har manipulerats. Sverige har genom Internetstiftelsen varit drivande i implementeringen av DNSSEC och det erbjuds sedan 2007 till alla innehavare av .se-domäner. Däremot har inte domännamnsinnehavarna implementerat DNSSEC i lika stor utsträckning. Det saknas tillräcklig statistik för att svara på exakt hur stor andel av de svenska domännamnen som har implementerat DNSSEC, men enligt statistik över de mest besökta domänerna så stöds det av 32 procent av .se-domänerna.[128] När det gäller svenska myndighetsdomäner visar en sammanställning att DNSSEC är aktiverat för 148 myndighetsdomäner och att flertalet myndigheter inte har det aktiverat.[129] Sverige ligger relativt högt i Europa med 85 procent validering av domänuppslag.[130]

Internet Protocol version 6 (IPv6)

Allt som kopplas upp mot internet måste ha en IP-adress för att fungera. IPv6 är den senaste versionen av protokoll som låter internetansluten utrustning

[125] https://defence-industry-space.ec.europa.eu/iris2-european-commission-awards-concession-contract-spacerise-consortium-2024-10-31_en
[126] https://www.enisa.europa.eu/sites/default/files/all_files/RPKI%20-%20ENISA%20-%20May%202024%20-%20To%20upload.pdf
[127] Netnod ansvarar för driften av rotnamnservertjänsten för I-roten sedan 2000, https://www.netnod.se/i-root/i.root-servers.net
[128] https://ec.europa.eu/internet-standards/dns.html#globan-dropdown-jk58gztmxgb
[129] https://www.myndighetermeddnssec.se/
[130] https://ec.europa.eu/internet-standards/dns.html#globan-dropdown-jk58gztmxgb

kommunicera med varandra. IPv6 ersätter den tidigare standarden IPv4 och innebär att betydligt fler enheter kan kopplas upp mot internet och tilldelas en publik IP-adress. Protokollet medger även flera andra tekniska säkerhetsfördelar.

PTS har haft ett antal regeringsuppdrag under årens lopp sedan 2010 om att främja införandet av IPv6 inom främst offentlig sektor. Främjandet av IPv6-införande i den offentliga sektorn har även setts kunna göra synergieffekter som även ska leda till ett allmänt bredare införande av IPv6 generellt i de allmänna elektroniska kommunikationsnäten i Sverige. Sedan 2022 har PTS främjandearbete primärt bestått i att samla marknadens och andra aktörer genom IPv6-forum där olika teman kopplats till IPv6-adressering har presenterats och diskuterats.

PTS har tagit fram en praktisk vägledning som hjälper it-avdelningen att planera, införa och förvalta IPv6. Vägledningen är avsedd för den offentliga sektorn men är stora delar även tillämplig för den privata sektorn. PTS har också tidigare tagit fram en vägledning till beslutsfattare inom den offentliga sektorn för att skapa en medvetenhet om nyttan med att påbörja införandet av IPv6 inom den sektorn.

I genomförandeförordning till NIS 2-direktivet finns krav på att ha en plan på att implementera IPv6. Genomförandeförordningen gäller dock endast en delmängd av aktörerna som omfattas av NIS 2 men ska ändå ses som vägledande.

Analys av nuläget

Sverige har en överlag välutbyggd internetinfrastruktur som täcker nästan hela Sverige. Nationella telesamverkansgruppen, med representation från både myndigheter och centrala privata aktörer, ökar förmågan att hantera allvarliga samhällsstörningar genom samordning av berörda parter. Det finns vidare väletablerade nätverk och samverkansfora för verksamheter som tillhandahåller internetinfrastruktur. Ansvarsförhållandena vad gäller nätens drift, underhåll och reparation i fredstid och ordinära krissituationer är förhållandevis tydliga i ljuset av lagregleringen, ansvarsprincipen och existerande föreskrifter. Den nya cybersäkerhetslagen förväntas vidare förstärka den öppna kärnans motståndskraft ytterligare genom utökad kravställning.

Nationella stamnät

Säkerhets- och driftkraven på stamnäten i Sverige är höga enligt gällande föreskrifter. De nationella stamnäten är emellertid uppkopplade till ett begränsat antal internationella anslutningar. Detta skapar ett beroende till andra stater och kommersiella utländska aktörer och kan påverka förmågan att säkerställa tillräcklig redundans.

Undervattenskablar

Redundansen i den digitala undervattensinfrastrukturen är god och bidrar till tillgängligheten i den offentliga kärnan i händelse av kabelbrott. Det finns internationella samarbeten inom Nato och EU, samt multilaterala initiativ på olika nivåer, vilket bidrar till att förmågan att hantera incidenter och sabotage och skapar resiliens i undervattenskabelsystemet. Det är positivt att åtgärder redan genomförts eller påbörjats under 2025 för att komma tillrätta med identifierade brister MCF:s redovisning av regeringsuppdrag Fö2025/00713. Följande förbättringspunkter har identifierats:

- I slutredovisningen av regeringsuppdrag Fö2025/00713 konstaterades att förmågan att hantera incidenter och säkerställa informationsförsörjning behöver stärkas. Samordningsförmågan behöver stärkas för att hanteringen av händelser ska bli mer effektiv. Försvarsmakten belyser bland annat i sina kommentarer till Fö2025/00713 att åtgärdsförslagen på ett tydligare sätt bör redogöra för *hur* förmågan i det civila försvaret att upptäcka incidenter och störningar kan höjas.
- Det råder brist på svenska fartyg som kan reparera undervattenskablar. Detta innebär att det kan ta lång tid att laga kablar om flera skulle kapas parallellt i händelse av konflikt eller krig.

Satellitkommunikation

IRIS² kommer förbättra tillgängligheten till säkra satellitkommunikationer i hela EU. Systemet kommer dessutom vara anpassat för militära behov och krissituationer för att stärka motståndskraften och tillgängligheten vid extraordinära händelser. En unionsgemensam satellitkonstellation skapar redundans och minskar beroendet av andra aktörer för alternativa kommunikationsmedel vid avbrott i andra delar av den digitala infrastrukturen. Följande brister har identifierats:

- Sverige är i hög grad beroende av utländska kommersiella tjänster för satellitbaserad internetkommunikation. Detta utgör en sårbarhet eftersom sådana tjänster kan stängas av till följd av exempelvis politiskt tryck och Sverige kan således förlora stora delar av förmågan i kristider.

BGP

Det är positivt att PTS tillsyn 2021 medförde att samtliga stora operatörer införde RPKI. Implementeringen av RPKI är enligt statistiken lägre än i många andra EU-länder och kan ökas ytterligare.

DNS

Sverige har en rotserver för DNS och har därmed inte något externt beroende för tillgång till listor över auktoritativa namnservrar. Detta medför goda förutsättningar för organisationer att införa DNSSEC. Följande sårbarhet har identifierats:

- Organisationer implementerar inte alltid DNSSEC. Detta gör DNS mer sårbart för angrepp och handhavandefel, vilket kan påverka integriteten i den offentliga kärnan. Orsaken till detta är att säkra DNS-lösningar kan vara kostsamma och komplicerade att införa.

IPv6

Införandet av IPv6 går långsamt framåt, men ökningar har skett inom offentlig sektor.[131] IPv6 behövs för fortsatt digitalisering och säker och tillgänglig kommunikation.

Det finns idag inga svenska offentligrättsliga regelverk avseseende generellt införande IPv6 för de allmänna näten eller specifika krav offentlig sektor. PTS ser dock reglering på området som en önskvärd väg framåt.

Målbild 2029

Sverige har fortsatt en välutbyggd och tillgänglig internetinfrastruktur som når alla medborgare och organisationer oberoende av teknikskiften. Motståndskraften i det öppna internets offentliga kärna är fortsatt god och har stärkts ytterligare. Det finns fortsatt tydliga ansvarsförhållanden vid avbrott i den digitala infrastrukturen. Etablerade och välfungerande samarbeten upprätthålls för att hantera incidenter.

Sverige har 2029 en tydlig reglering och effektiv tillsyn av de aktörer som är viktiga för internets öppna kärna.

Redundansen i undervattenskabelinfrastrukturen är fortsatt god. Det finns etablerade rutiner mellan berörda offentliga och privata aktörer för att effektivt kunna inrikta, samordna och ta fram en gemensam sjölägesbild vid incidenter kopplade till undervattenskablar. Förmågan att skyndsamt kunna reparera undervattenskabelsinfrastruktur för digital kommunikation har stärkts.

Sverige har egna markstationer för satellitkommunikation och skapat nödvändiga förutsättningar för att kunna börja nyttja IRIS² som redundans vid avbrott i kabelinfrastrukturen.

DNSSEC är implementerat i hela den offentliga sektorn och hos majoriteten av domännamnsinnehavarna. RPKI är implementerat i hela den offentliga sektorn

[131] Se PTS webbtjänst: https://www.ipv6ioffentligsektor.se/

och av åtminstone 90 procent av verksamhetsutövare i privat sektor. Samtliga statliga myndigheter, kommuner och regioner har infört IPv6 i relevanta delar av it-infrastrukturen. Tillhandahållare av fasta och mobila elektroniska kommunikationsnät erbjuder IPv6 i sina elektroniska kommunikationsnät och tjänster.

Åtgärder för att uppnå målbilden

1. Tillsynsmyndigheterna ska ta fram föreskrifter i enlighet med cybersäkerhetslagen och cybersäkerhetsförordningen. De ska utöva relevant tillsyn över och ge vägledning till verksamhetsutövare som omfattas av regleringen. Verksamhetsutövare som omfattas av regleringen ska följa lagstadgade krav och gällande föreskrifter. PTS kommer under 2026 att ta fram nya föreskrifter och börja genomföra tillsyn enligt dessa föreskrifter. PTS kommer vidare utreda behovet av att ytterligare förstärka motståndskraften och redundansen i den offentliga kärnans fysiska infrastruktur på land (nationella stamnät och noder), i vatten (undervattenskabelinfrastruktur) och i rymden (satellitkommunikation).

2. Statliga och privata aktörer ska hålla regelbundna och behovsstyrda gemensamma övningar för att stärka incidenthanteringen.

3. Åtgärderna för incidenthantering vid avbrott i undervattenskabelinfrastrukturen, som föreslås av Myndigheten för civilt försvar och Försvarsmakten i redovisningen av regeringsuppdrag 2025/00713, bör utredas vidare och implementeras utifrån vad som anses lämpligast utifrån ett totalförsvarsperspektiv. PTS ska utreda hur förmågan att reparera undervattenskablar och tillgången till reparationsfartyg kan säkerställas för svensk del i fredstid, kris och väpnad konflikt.

4. PTS ska arbeta för att främja Sveriges integration i IRIS² inför den planerade lanseringen av tjänsten 2030.

5. Samtliga statliga myndigheter, kommuner och regioner ska få en skyldighet att införa DNSSEC och RPKI.

6. Samtliga statliga myndigheter, kommuner och regioner ska få en skyldighet att införa IPv6 i relevanta delar av sin it-infrastruktur. Tillhandahållare av fasta och mobila elektroniska kommunikationsnät ska få en skyldighet att erbjuda IPv6 i sina elektroniska kommunikationsnät och tjänster.

Indikatorer

Referenser

Utveckling och integrering av ny cybersäkerhetsteknologi

Enligt NIS 2-direktivets artikel 7.2 e) Riktlinjer för att främja utveckling och integrering av relevant avancerad teknik som syftar till att genomföra moderna riskhanteringsåtgärder för cybersäkerhet.

Definitioner och begrepp

Avancerad teknik: Metoder som bygger på den senaste forskningen, använder sofistikerade angrepps- eller försvarsmekanismer och kräver expertis för att utveckla.

Artificiell intelligens (AI): Ett datorsystems förmåga att utföra en definierad uppgift bättre än en människa.

Bakdörr: En dold eller icke-dokumenterad mekanism som ger systemåtkomst på annat sätt än avsett och innebär således en säkerhetsrisk.

Blockkedjeteknologi: En distribuerad databas som lagrar information i en kedja av block. Varje block innehåller en lista över transaktioner, tidsstämpel och referens till föregående block. Strukturen gör det svårt att manipulera informationen.

Compliance-appar: Programvara som kan stötta organisationer att följa lagar och standarder inom cybersäkerhet och dataskydd, såsom GDPR och PCI-DSS. De säkerställer riskhantering, dataskydd och dokumentation för att upprätthålla efterlevnad och minimera juridiska konsekvenser.

Interoperabilitet: Två eller flera systems förmåga att utbyta information och att använda informationen som de får från varandra.

Kaskadangrepp: När en lyckad kompromettering i en leveranskedja utnyttjas för att genomföra ytterligare en leveranskedjekompromettering i nästa led. Detta innebär att intrånget kedjar vidare mellan leverantörer eller produkter och till sist når slutkunden.

Kvantsäker kryptografi: Moderna kryptografiska lösningar som är utvecklade för att fortsatt skydda information när kvantdatorer blir tillräckligt kraftfulla för att bryta dagens metoder för asymmetrisk kryptografi.

Maskininlärning (ML): En delmängd av AI som använder matematiska modeller för att hjälpa datorer att lära sig från data utan direkt instruktion.

Mjukvaruförteckning (SBOM): En detaljerad förteckning över vad som ingår i ett mjukvarusystem.

Phishing: En form av bedrägeri där en e-postavsändare försöker imitera en legitim aktör i antagonistiskt syfte.

Stora språkmodeller (LLM): En avancerad typ av AI som är tränad på mycket stora mängder textdata för att kunna förstå, sammanfatta, generera och förutsäga nytt innehåll

Teknikagnostisk: Refererar till en inställning som är oberoende av specifika tekniska lösningar och fokuserar på att välja den mest effektiva teknologin för ett visst behov.

Zero-Trust arkitektur: En säkerhetsstrategi som eftersträvar att minimera tillit och som bl. a kräver kontinuerlig autentisering av användare.

Introduktion

Detta policyområde behandlar hur Sverige ska säkerställa ett systematiskt och långsiktigt förhållningssätt till avancerad cybersäkerhetsteknik med utgångspunkten att avancerade tekniska lösningar finns men att verksamheters förmåga att ta dem i bruk varierar. Organisationer ska även ges möjligt att delta i utveckling, anpassa sig till förändrade arbetssätt och nya tekniker då hotbilden förändras i hög takt. Policyn fokuserar därför inte på enskilda tekniker, utan på hur Sverige organiserar sin förmåga att upptäcka, förstå, värdera och införa ny avancerad teknik som ett modernt riskhanteringsstöd.

Policyn bygger på två kompletterande förhållningssätt:

1. **Avancerad teknik för moderna riskhanteringsåtgärder**
   Detta förhållningssätt betonar att Sverige behöver:
   - kontinuerligt följa och analysera utvecklingen av ny avancerad cybersäkerhetsteknik,
   - säkerställa att relevant forskning, utveckling och innovation tas tillvara nationellt, och
   - omsätta både nya och redan etablerade tekniska metoder till praktiskt bruk i svenska verksamheter.

Fokus ligger på att skapa förmågor för att *införa, integrera och drifta teknik* som gör riskhanteringen mer proaktiv, datadriven och robust.

2. **Initiativ och samarbete inom Sverige och EU**
   Detta förhållningssätt betonar att Sverige behöver agera som en del av ett större ekosystem, där utvecklingen av avancerad cybersäkerhetsteknik påverkas av EU-regelverk, internationella säkerhetsstandarder och samarbete i olika forum. Policyn riktar därför in sig på:

- nationell samordning och kunskapsdelning,
- deltagande i internationella program, testbäddar och standardiseringsprocesser,
- och systematisk återföring av internationella erfarenheter till svenska riktlinjer och verksamheter.

Tillsammans skapar dessa två förhållningssätt en modell där Sverige både håller jämna steg med teknikutvecklingen och har strukturer för att snabbt omsätta ny kunskap till avancerad operativ cybersäkerhetsförmåga. Denna operativa förmåga behöver dock beakta digital suveränitet, omvärldsläget samt legala krav vid utveckling och implementering av avancerad teknik.

Avgränsning

Denna policy (7.2e) fokuserar på utveckling, införande och integrering av avancerad teknik (t.ex. AI, ML, Zero Trust, kvantsäker kryptografi, avancerad logganalys,) för moderna riskhanteringsåtgärder. Policyn är teknikagnostisk och behandlar *hur* tekniken tas i bruk. Policyn behandlar inte detaljerad kravställning, upphandling eller allmän cyberhygien.

Nulägesbild

Under 2025 har det globalt skett en betydande ökning av incidenter, exempelvis har ransomwareangrepp[132] ökat kraftigt[133]. Tillgänglig svensk statistik[134] synliggör att en stor del av incidenterna orsakas av mänskliga misstag (22 procent) och systemfel (27 procent), och över hälften av alla inkomna incidenter uppges ha skett hos en leverantör, där insyn ofta är begränsad. Flera incidenter i närtid visar på ett behov av nyttjande av avancerad teknik inom cybersäkerhet. Sådana incidenter har exempelvis rört felaktiga uppdateringar som orsakat globala störningar, omfattande bedrägerier genomförda med stöd av AI och kaskadangrepp där ett angrepp på leverantörer förs vidare i leveranskedjan. I dagsläget finns avancerad teknik tillgänglig inom cybersäkerhet. Exempelvis ger maskininlärning verksamheter förmågan att upptäcka och svara på hot i realtid, på en skalnivå och grad av komplexitet som inte är möjlig för människan. Det innebär att AI, maskininlärning och stora språkmodeller hjälper verksamheter att upptäcka hot, hantera stora datamängder, minska falsklarm och kontinuerligt anpassa sig till nya attackmönster. Kvantsäker kryptering säkrar verksamheters krypterade information från kvantdatorer och olika tekniker inom Zero Trust-arkitektur, med kontinuerlig verifiering och multifaktorsautentisering, minskar

[132] Ransomware (från engelskans ransom, lösen) är en slags programvara som låser (ofta genom kryptering) offrets data eller system och kräver *lösen*.
[133] https://blog.checkpoint.com/research/global-cyber-attacks-surge-in-october-2025-amid-explosive-ransomware-growth-and-rising-genai-threats/
[134] Uppdateras med nya siffror när senaste rapporten finns tillgänglig

risken för intrång och dataläckor. Sammanfattningsvis finns det en uppsjö av avancerad teknik för att verksamheter ska kunna stå emot moderna cyberhot.

Trots att avancerad teknik finns tillgänglig nyttjas den av svenska verksamheter i begränsad utsträckning.[135] Svenska verksamheter har förvisso börjat nyttja AI i en relativt sett hög utsträckning[136], men användandet av avancerad teknik inom cybersäkerhetsarbetet är begränsad. Att avancerad teknik inte är implementerad eller används i otillräcklig utsträckning kan indikera att verksamheter ännu inte har den styrning, mognad eller kompetens som avancerad teknik kräver, vilket i sin tur kan innebära att den avancerade tekniken implementeras felaktigt så att den inte får avsedd effekt.[137] Begränsande faktorer i sammanhanget är till exempel äldre, utdaterade digitala system, som inte är kompatibla med- eller är svåra att integrera tillsammans med ny teknik. Det finns flera exempel på att utdaterad teknik kan bromsa digital transformation.[138]

Utveckling och integrering av avancerad teknik i Sverige

Sverige har under de senaste åren intensifierat arbetet med att integrera avancerad teknik i det nationella cybersäkerhetsarbetet. Flera myndigheter, forskningsaktörer och företag bedriver samverkansinitiativ för att stärka förmågan att upptäcka, förebygga och hantera cyberangrepp. Dessa satsningar speglar en hög innovationskraft och en växande förståelse för att teknik behöver användas mer systematiskt och integreras i verksamheters riskhantering. I Sverige pågår ett parallellt arbete för att stödja aktörer i att uppfylla ställda krav och höja den tekniska grundnivån.

Regelverk och initiativ

EU:s regelverk driver på ett bredare införande av avancerad teknik i medlemsstaterna vilket NIS 2 tydligt ställer krav på. Cyberresiliensförordningen (CRA) stärker de krav som ställs på produkter med digitala inslag, bland annat genom krav på programvaruförteckningar, detaljerade listor över alla komponenter som ingår i en mjukvara (SBOM) och spårbarhet i leveranskedjor och verifierbarhet av programvara, vilket förutsätter tekniska lösningar för komponentinventering och signaturhantering.

[135] Se exempelvis Cybersäkerhetskollen 2024. Uppdateras efter rapportsläpp 27/2
[136] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises
[137] MSB:s årsrapport – Incidentrapportering 2024.
[138] Irani, Z., Abril, R.M., Weerakkody, V., Omar, A. and Sivarajah, U., 2023. The impact of legacy systems on digital transformation in European public administration: Lesson learned from a multi case analysis. *Government Information Quarterly*, *40*(1), p.101784.

EU:s färdplan för post-kvantumkryptografi (PQC) innebär att organisationer successivt måste migrera till kvantsäkra algoritmer. Detta visar tydligt hur EU-ramverk accelererar införandet av specifika tekniktyper i Sverige.

AI-förordningen ställer därtill krav på säker användning av AI, där teknisk modellövervakning, datastyrning och loggning är nödvändiga för efterlevnad.

EU:s cybersäkerhetscertifieringar (EUCC) ställer krav på robust kryptografi, kontinuerlig övervakning och säker hantering av identiteter – områden där avancerad teknik utgör den praktiska möjliggöraren.

Nationellt regelverk och strategi

Sverige har genom Cybersäkerhetslagen och kompletterande myndighetsföreskrifter etablerat ett regelverk som ställer högre krav på verksamhetsutövare att använda avancerad cybersäkerhetsteknologi. Inom kontinuerlig riskanalys, incidenthantering, loggning, säkerhet i leveranskedjor samt styrning av utveckling och drift stärks kraven betydligt när det gäller tekniska lösningar för exempelvis logganalys, automatiserad händelsekorrelation och övergång till kvantsäker kryptografi (PQC).

Den ökade resurstillförseln på området förbättrar förutsättningarna för implementering men understryker samtidigt behovet av tydligare stöd för hur tekniken ska införas och integreras.

EU-standarder

Idag har Sverige ett stort engagemang inom EU i utvecklingen av tekniktunga standarder, såsom övergång till kvantsäker kryptografi (PQC). Berörda statliga myndigheter, i samarbete med näringslivet, verkar bland annat för att nya standarder och europeiska certifieringsordningar för cybersäkerhet utvecklas transparent samt att svenska behov och prioriteringar får genomslag.

Standardisering är avgörande för tekniskt ledarskap och för utveckling av säkra digitala tekniker, infrastruktur och säkra leveranskedjor. Sverige verkar för ökat engagemang i standardiseringsprocesser som kan bidra till att motverka marknadshinder, främja innovation och stimulera ekonomisk utveckling. Det internationella standardiseringsarbetet är dock generellt inget som drivs genom myndigheter förutom för specifika standardiseringsinitiativ samt inom den standardiseringsgrupp som finns inom NCSC för elektronisk kommunikation samt molntjänster. Sverige är trots detta en stark aktör som flera av våra grannländer lutar sig mot när det gäller exempelvis ledningssystemstandarderna inom ISO 27000 serien tack vara ett stort ideellt engagemang via Teknisk Kommitté 318-informationssäkerhet, cybersäkerhet och integritetsskydd (SIS TK 318)[139]. Det

[139] https://www.sis.se/delta-och-paverka/tksidor/tk300399/sistk318/

finns ett behov samt potential för fördjupat samarbete inom områden som exempelvis AI, kryptografi och elektronisk kommunikation.

Samordning och strategiska initiativ från myndigheter för utveckling av standarder som stöd för avancerad teknik saknas. Användningen av internationella och väletablerade standarder framförs ofta som lämpligt i nationella föreskrifter (se exempelvis MSBFS 2020:6 och MSBFS 2020:7) och vägledningar samt organisationers egna styrning och riktlinjer och som indirekt styr implementering och användning av avancerad teknik. Cybersäkerhetskollen, som mäter nivån på verksamheters systematiska cybersäkerhetarbete, visar att det är en utmaning att mäta implementeringen, både när det gäller den övergripande organisatoriska styrningen av det systematiska arbetet och de specifikt utformade tekniska standarderna. Resultaten understryker att engagemang från ledningen och strukturerad uppföljning är avgörande för att säkerställa att dessa delar får genomslag i praktiken där standarder kan ge stöd för systematik och ledningsprocesser.

Analys av nuläget

Avancerad teknik, såsom AI och maskininlärning, kan nyttjas för att stärka cybersäkerhetsarbetet och höja säkerheten inom verksamheter. Det är emellertid utmanande att avancerad teknik möjliggjort en betydande ökning av alltmer sofistikerade cyberangrepp[140]. Upprepade högprofilerade incidenter minskar medborgarnas tillit till digitala system och kan bromsa nödvändig digitalisering. Avancerad teknik förebygger och minskar risken för att incidenter inträffar och mildrar dessutom dess konsekvenser.

God tillgång till avancerad teknik inom Sverige skapar förutsättningar för verksamheter att implementera lämpliga, proportionerliga säkerhetsåtgärder för att möta aktuella hot. Det är emellertid otillfredsställande att användandet och implementeringen av avancerad teknik endast sker i begränsad utsträckning i Sverige. Svenska verksamheter bör ha möjlighet att fullt ut utnyttja avancerad teknik för att maximera dess fördelar. Ett problem är att implementeringen av avancerad teknik inte sker i den takt som är nödvändig för att möta hotbilden, trots att tekniken i sig finns tillgänglig, reglering är på plats och resurser för initiativ till avancerad teknik allokeras nationellt. Orsaker till detta kan bero på:

- Äldre system och teknisk skuld. Stora delar av den befintliga infrastrukturen är inte anpassad för integration med modern teknik, vilket gör migrering tids- och resurskrävande, särskilt då många system saknar stöd för modern identitets- och åtkomsthantering, centraliserad loggning eller automatiserade säkerhetskontroller. Detta kan delvis förklaras genom att inköp och införande av nya system ofta innebär en betydande kostnad

[140] ENISA Threat Landscape Report 2025

och kräver teknisk kompetens, samtidigt som de äldre systemen ofta inneburit en större investering. Den samlade konsekvensen av detta är kvarlevande äldre tekniska system med tillhörande integrationsproblematik.

- Brist på kompetens och långsiktighet utgör ett betydande hinder för effektiva verksamheter. Många organisationer saknar specialistkompetens när det gäller att välja, driftsätta och förvalta avancerad teknik. Detta förvärras av att cybersäkerhetsarbetet ofta bedrivs i projektform, vilket hindrar en långsiktig och hållbar förvaltning. Utan en strategisk ledningsförmåga att planera för livscykelhantering missas möjligheten till kontinuerlig uppdatering och drift över tid. Dessutom leder denna brist på strategisk planering till osäkerhet kring ansvar för modellunderhåll och teknikuppgraderingar, vilket i sin tur kan resultera i sårbarheter och ineffektivt resursutnyttjande.

Utveckling och integrering av avancerad teknik i Sverige

Sverige har ett starkt och tydligt regelverk genom Cybersäkerhetslagen, AI-förordningen och Cyberresiliensförordningen (CRA). Regelverket skapar tydliga krav gentemot verksamhetsutövare som i praktiken förutsätter utveckling och användning av avancerad teknik.

Många verksamheter har ännu inte de processer eller den tekniska grund som krävs för att uppfylla regelverkens krav på kontinuerlig övervakning, spårbarhet och teknisk robusthet. Behovet av fortsatt samverkan mellan myndigheter, akademi och näringsliv är viktigt för att kunna öka implementeringen.

Flera faktorer bidrar till gapet mellan krav och faktisk teknikadoption:

- Regelkraven är tekniskt komplexa och funktionsbaserade. Många verksamheter saknar verktyg, kompetens och vägledande referensmönster för att tolka och omsätta kraven i arkitektur och kontroller (t.ex. SBOM/CRA, säkerhetsloggning/NIS 2, AI-krav och PQC). Konsekvensen är ojämn och sen implementering: åtgärder drivs som piloter/projekt, lösningar blir svårjämförbara mellan aktörer och tiden från krav till implementering ökar, vilket försvårar tillsyn, interoperabilitet och effektiv riskreduktion[141]

- Avsaknad av nationellt standardiserade lösningar innebär att organisationer utvecklar egna tekniska tillvägagångssätt. Detta leder till

[141] Upphandlings- och leverantörskrav behandlas i policyområdena för leveranskedjor och cybersäker upphandling; forsknings- och innovationsstöd behandlas i policyområdet för utbildning, forskning och innovation.

bristande interoperabilitet, begränsat erfarenhetsutbyte och svårigheter att skala från pilot till förvaltad förmåga, eftersom certifierade produkter, gemensamma referensarkitekturer, tekniska mönster och nationell vägledning saknas.

Regelverk och initiativ

Regleringarna på EU- och nationell nivå driver tydligt fram behovet av tekniska lösningar. EUCC, CRA och PQC-färdplanen sätter en teknisk ambitionsnivå som skapar förutsägbarhet för verksamheterna, samtidigt som de i praktiken förutsätter användning av avancerad teknik för att säkerställa efterlevnad. Svenska myndigheter har tagit fram flera stödmaterial och nationella satsningar för att underlätta införandet. Dessa initiativ bidrar till att Sveriges digitala infrastruktur successivt kan stödja driftsättning av avancerad teknik i större skala, inte enbart som skyddsåtgärder i sig, utan även som möjliggörare för annan digital utveckling och införande av ny teknik på ett säkert och kontrollerat sätt. Sammantaget skapar regelverken ett läge där avancerad teknik inte är ett val, utan en förutsättning för praktisk regelefterlevnad och för att verksamheter ska kunna ta tillvara ny teknik utan att öka riskexponeringen.

För att kunna utgå från en standardiserad grund där tekniska lösningar tas fram på ett hållbart och internationellt beprövat sätt krävs att Sverige deltar i internationella standardiseringsarbeten. Detta är särskilt viktigt för avancerad cybersäkerhetsteknik, då gemensamma standarder och tekniska ramverk minskar trösklarna för införande och gör det möjligt att återanvända lösningar mellan verksamheter och sektorer. Detta skapar även grund till kompetens inom området, eftersom både regelverk, tekniska lösningar och tillämpningspraxis utvecklas parallellt. Avsaknad av samordnad nationell styrning och prioritering för deltagande i internationella standardiseringsarbeten innebär att svenska myndigheters medverkan i dag är ojämn och i stor utsträckning personberoende. Detta begränsar Sveriges möjligheter att påverka utformningen av standarder för avancerad cybersäkerhetsteknik och försvårar ett likvärdigt och effektivt införande nationellt.

Regeringens satsningar på cybersäkerhet, bland annat genom Cybersäkerhetsmiljarden[142], visar att cybersäkerhet är ett prioriterat område vilket skapar förutsättningar för investeringar i avancerad teknik. Att verksamheter får tillgång till statliga satsningar, finansiering och gemensamma initiativ som minskar både kostnads- och risktrösklar för införande av avancerad cybersäkerhetsteknik kan ses som en möjliggörare för ökad implementering av avancerad teknik. Investeringar och resursallokering är avgörande för att uppnå organisatoriska mål med stöd av tekniska lösningar. Eftersom dessa beslut typiskt ligger på

[142] https://www.regeringen.se/pressmeddelanden/2025/09/nationell-satsning-pa-cybersakerhet/

ledningsnivå, kan man indirekt dra slutsatsen att ledningens engagemang och förståelse för avancerad teknik är viktig för att uppnå viktiga strategiska mål. Detta korrelerar med högre teknikadoption. Utan aktivt stöd från ledningen riskerar organisationen att stanna vid strategiska ambitioner, utan att praktiskt implementera dem. Sveriges teknikintensiva näringsliv samt samverkan mellan akademi och industri skapar ett starkt innovativt svenskt teknologiskt försprång.

Verktyg och processer för att nå målen saknas ofta, särskilt på områden där krav ställs på logganalys, spårbarhet, kontinuerlig övervakning och PQC-migrering.

- Implementeringstakten för nya regelverk är betydligt lägre än den snabba utvecklingstakten i ställande krav från NIS 2, CRA och AI-förordningen. Detta innebär att många verksamheter kämpar med att hinna i kapp, vilket kan leda till att de inte kan säkerställa regelefterlevnad och därmed riskerar rättsliga och operationella konsekvenser.

- Bristen på integrerade arbetsmetoder resulterar i ineffektiva processer för införande, förvaltning och uppföljning av avancerad teknik. Utan etablerade rutiner, särskilt i mindre organisationer, försvåras implementeringen och leder till missade möjligheter att optimera verksamheten.

- Resurs- och kompetensbrist försvårar situationen ytterligare. Många verksamheter har varken den nödvändiga finansieringen eller personal med den tekniska kompetens som krävs för att navigera den snabbt föränderliga teknologiska miljön, vilket kan leda till allvarliga säkerhetsrisker och ineffektiv drift.

- Den tekniska miljöns komplexitet försvårar också införandet av modern teknik. Äldre system och fragmenterade it-miljöer gör det ofta svårt att implementera nya lösningar utan omfattande omställningar, vilket kan leda till fördröjningar, ökade kostnader och ineffektivitet i verksamheten.

- Med EU:s mål om post-kvantumkryptering senast 2030 har Sverige fem år på sig att migrera kritiska system.

Eskalerande hot

Samhällets digitalisering och snabba teknologiska utveckling har skapat både möjligheter och risker. De senaste åren har hotbilden ökat väsentligt, med försämrat säkerhetsläge, snabbt växande antal cyberangrepp mot offentlig och privat sektor och hotaktörer, med stöd av avancerad teknik, som utför mer omfattande och automatiserade cyberangrepp. En konsekvens av detta är att stora

delar av det traditionella arbetssättet, inom cybersäkerhet, inte längre kan hantera dessa risker på ett proaktivt sätt[143].

Cybersäkerhetsarbetet innebär att i ökad utsträckning genomföra riskanalyser och informationsklassningar för att bedöma lämpliga och proportionerliga säkerhetsåtgärder med utgångspunkt i identifierade risker och informationstillgångars skyddsvärde. I och med att den teknologiska utvecklingen har möjliggjort användande av avancerad teknik såsom AI i samband med cyberangrepp genom exempelvis AI-genererad skadlig kod och automatiserade angrepp, har detta lett till att motsvarande avancerad teknik används inom cybersäkerhet, för att möta de ökade cyberhoten som den tekniska utvecklingen medför.

Målbild 2029

Privat-offentlig samverkan

Sveriges starka regleringsram genom Cybersäkerhetslagen, AI-förordningen och Cyberresiliensförordningen samt tillgången till avancerad cybersäkerhetsteknik är fortsatt en tillgång 2029. Samverkan mellan offentlig sektor, akademi och näringsliv fortsätter att skapa goda förutsättningar för att ta fram och nyttja ny avancerad teknik som skyddsåtgärder.

Ökad grad av implementering

2029 har nulägets ojämna implementering ersatts av ett brett införande av avancerad teknik där minst 70 procent av verksamhetsutövare enligt Cybersäkerhetslagen (NIS 2) uppnår minst nivå 3 i Cybersäkerhetskollen för tekniknära förmågor, vilket i praktiken innebär att verksamheterna kan påvisa att centraliserad loggning med korrelation används för prioriterade system, att grundläggande Zero-Trust-principer tillämpas i verksamhetskritiska miljöer samt att det finns en tidsatt plan för övergång till post-kvantumkryptografi för de mest skyddsvärda informationsflödena.

Minskad teknisk skuld och bättre resursutnyttjande

Den resurstillförsel som beslutas för cybersäkerhetsområdet är i proportion till aktuella hot och risker samt säkerställs långsiktigt genom fleråriga regeringsöverskridande överenskomna budgetramar. Den tekniska skulden på samhällsnivå minskar genom stödinsatser som möjliggör implementering av avancerad teknik.

[143] Se Mohamed, N., 2025. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, pp.1–87.

Stärkt forskning och innovation

År 2029 har forskning- och innovation på cybersäkerhetsområdet stärkts. Den ämnesbundna forskningsfinansieringen har möjliggjort cybersäkerhetsforskning och NCC-SE har i utökad grad bidragit med både generellt och individualiserat stöd till aktörer att söka medel genom EU-program som Horisont och DIGITAL. NCC-SE har tillsammans med Cybercampus och Cybernoden bidragit till att underlätta ekonomiskt stöd till medfinansiering vilket gjort det väsentligt lättare för intressenter att ansöka till utlysningar inom EU. Ett stadigt ökande antal aktörer har sökt och fortsätter söka både EU- andra internationella medel. Sverige är fortsatt aktiva i att påverka innehåll i arbetsprogram för kommande utlysningar i ett tidigt skede genom samverkan mellan bland annat de nationella initiativen och regeringskansliet.

Tillämpning av standarder och certifieringar

EU:s gemensamma standarder och certifieringssystem tillämpas fullt ut. NCSC bevakar och påverkar internationell standardisering i samarbete med nationellt standardiseringsorgan och samverkar med CSEC[144] som utövar tillsyn.

Minskning av mänskliga misstag och införande av Zero Trust-arkitektur

De mänskliga misstag och systemfel som tidigare angetts som orsak i hälften av alla incidentrapporter har genom omfattande automatisering av rutinuppgifter och systemövervakning reducerats till under 10 procent. Principen om kontinuerlig verifiering och nolltolerans för implicit förtroende, som var begränsat implementerad, är nu standard i alla statliga myndigheter och över häften av kommuner och regioner.

Ökade krav på programvarudeklarationer

År 2029 ställs krav på transparent dokumentation av programvarukomponenter, verifierbar riktighet och systematisk incidentdelning mellan kund och leverantör. Denna kravställning bidrar till säkrare leveranskedjor och transparanta leverantörsrelationer.

Automatiserat stöd för regelefterlevnad och framtidssäkrad kryptering

2029 har Sverige slutfört övergången till framtidssäkrad kryptografi som möter dagens och kommande kvantrelaterade hot. Den manuella och tidskrävande

[144] Sveriges Certifieringsorgan för IT-säkerhet (CSEC) är en oberoende enhet inom FMV och verkar som Sveriges nationella certifieringsorgan för it-säkerhet i produkter och system.

regelefterlevnad som tidigare dominerade ersätts av långt mer automatiserade processer för övervakning, rapportering och uppföljning.

Enhetlig säkerhetsnivå

Genom nationellt styrda men regionalt placerade stödfunktioner säkerställs att även resursbegränsade organisationer får tillgång till avancerad cybersäkerhetsförmåga. Dessa regionala enheter fungerar som utlokaliserade nationella CSIRT-resurser och verkar enligt gemensamma nationella standarder, metoder och plattformar.

Samverkan mellan regionala aktörer och NCSC/CSIRT tillhandahåller i detta upplägg rådgivning, incidentstöd och samordning inom informationssäkerhet och kontinuitetshantering till kommuner och andra aktörer i respektive län, särskilt kopplat till det civila försvaret och totalförsvarsplaneringen. Funktionen kan förstärkas genom den Cyberreserv som etableras genom Cybersolidaritetsförordningen. På detta sätt ersätts fragmenterade lokala arbetssätt med en enhetligt styrd och nationellt koordinerad säkerhetsnivå i hela landet.

Omvärldsbevakning

2029 har Sverige etablerat en sammanhållen och systematisk omvärldsbevakning av avancerad cybersäkerhetsteknik ledd av NCSC. Till skillnad från nuläget, där omvärldsbevakning och internationell samverkan i stor utsträckning är fragmenterad och personberoende, kännetecknas 2029 av att omvärldsbevakningen är kontinuerlig, strukturerad och systematiskt omsatt i nationella analyser, vägledningar och rekommendationer. Syftet med omvärldsbevakningen är ett nationellt kunskapsunderlag för prioriteringar och teknikval. Lärdomar från omvärldsbevakningen används i nationella vägledningar och rekommendationer.

Internationella samarbeten

År 2029 finns ett internationellt samarbete för kunskapsdelning och utveckling av avancerad teknik. Samarbetet är väl utvecklat inte bara inom EU, utan även inom Nato och andra internationella forum där avancerad teknik och cybersäkerhetsfrågor behandlas. Sverige deltar aktivt i pilotprogram, testbäddar och standardiseringsarbetet inom såväl EU:s som Natos och andra internationella organisationers ramar.

Internationella standarder och ramverk

2029 utgör EU:s gemensamma standarder, certifieringssystem och tekniska ramverk grunden för avancerad teknik i Sverige). Sveriges internationella samarbete – i EU, Nato och övriga relevanta forum bidrar till ökad samordning,

gemensamma krav och snabbare tillgång till kunskap om standardiserad teknikutveckling.

Nationellt stärkt förmåga till regelefterlevnad

Sverige har 2029 etablerat förmågor för att snabbt införliva teknikrekommendationer från EU, Nato och andra internationella samarbeten i nationella vägledningar och kravdokument, vilket ger verksamheterna tydliga, aktuella och harmoniserade stöddokument som stödjer ett teknikagnostiskt och effektivt införande. Målet är att stödet används i tillsyn, strategiska teknikval eller initiativ som Sverige deltar i. Målbilden anses inte uppnådd om utveckling och teknikval fortsatt bedrivs ad hoc utan tydlig koppling till internationella krav och rekommendationer.

Åtgärder för att uppnå målbilden

Standardisering av tekniska lösningar

För att uppnå gemensamma standarder, referensarkitekturer och tekniska mönster som möjliggör skalning av avancerad teknik, effektiv tillsyn och certifiering samt ett likvärdigt och samordnat införande mellan verksamheter och sektorer, ska NCSC:s standardiseringsgrupp (som består av myndigheter med uppdrag att styra, rådge eller kontrollera säkerhet) i samverkan med SIS TK 318:

- Ta fram en strategi för vilka standardiseringsalternativ som ger förutsättningar för tekniska lösningar inom avancerade tekniska riskhanteringsåtgärder som Sverige ska delta i.

- Inrätta arbetsprogram med expertis som sammanställer processer för utveckling av avancerad teknik och användning av tekniska krav med hänvisning till internationella standarder. Arbetet med utveckling och implementering bör utgå från ett systematiskt arbetssätt motsvarande ISO 27001 samt vara riskbaserat med stöd av ISO 27005 och internationellt framtagna standarder för säkerhetsåtgärder. Arbetsprogram kan även krävas för tillsyn och revision där standarder såsom ISO 27007 och ISO 27008 kan användas som stöd. Syftet är att utveckla förmågan att kunna ställa krav på avancerad teknik och implementera den på rätt sätt.

För att genomföra detta krävs finansiering för deltagande av specialister, etablering och bemanning av arbetsprogram samt utveckling av standardiserade kompetensprofiler och certifierings- och/eller ackrediteringsprogram. Detta inkluderar etablering av en nationell prioritering för standardiseringsområden samt framtagande av gemensamma referensarkitekturer och tekniska mönster som kan användas av verksamhetsutövare och tillsyn för att möjliggöra ett enhetligt införande av avancerad cybersäkerhetsteknik.

Kompetenser och resurser

Tillräcklig kompetens och resurser är en grundförutsättning för samverkan, införande, drift och långsiktig förvaltning av avancerad cybersäkerhetsteknik, särskilt för verksamheter med begränsad egen kapacitet. För att säkra tillgången till kompetens och resurser ska NCSC i samverkan med UKÄ, MYH och lärosäten genom Cybercampus och regionala aktörer:

- Etablera strukturerade utbildningsprogram som säkerställer tillgång till kompetens för implementation, drift och främjande av moderna säkerhetslösningar.
- Inrätta regionala stödcenter som tillhandahåller delad expertis och tjänster för verksamheter med otillräcklig egen kapacitet.

För att genomföra detta krävs finansiering för utbildning av nödvändigt antal specialister, etablering och bemanning av regionala center samt utveckling av standardiserade kompetensprofiler och certifierings-/ackrediteringsprogram. Detta omfattar etablering av nationellt gemensamma kompetensprofiler för centrala nyckelroller samt regionala stödfunktioner som ger verksamheter praktiskt stöd vid införande och förvaltning av avancerad cybersäkerhetsteknik.

Nationell styrning

Tydlig nationell styrning, gemensamma principer och samordnade riktlinjer krävs för att möjliggöra samverkan, skalning från pilot till förvaltning, enhetliga arkitekturer och ett likvärdigt säkerhetsutfall. För att åstadkomma detta ska NCSC som samordnare i samverkan med tillsynsmyndigheter och SIS TK318:

- Utveckla nationella riktlinjer för implementation av moderna riskhanteringsåtgärder.
- Etablera gemensamma principer för säkerhetsarkitektur med fokus på kontinuerlig verifiering, segmentering och adaptiv riskhantering.

För att genomföra detta krävs resurser för vägledningar och implementeringsstöd, en etablerad samordningsfunktion samt juridisk översyn för att tydliggöra ansvar och befogenheter. Uppföljning behövs genom vidareutveckling av Cybersäkerhetskollen.

Hantering av tekniska sårbarheter som hindrar införande av avancerad teknik

System som inte kan moderniseras eller integreras med avancerade säkerhetslösningar utgör ett direkt hinder för både införande av modern identitets- och åtkomsthantering och centraliserad loggning eller automatiserade säkerhetskontroller samt övergång till framtidssäkrad kryptografi. För att åtgärda detta ska verksamhetsutövare med stöd från berörda myndigheter och NCSC:

- Genomföra moderniseringsprogram för att fasa ut system som inte kan skyddas effektivt.

- Införa automatiserad granskning och kontinuerlig säkerhetsanalys för alla systemförändringar.

För att genomföra detta krävs medfinansiering för modernisering av samhällskritiska system, tekniskt stöd för planering och genomförande av säker migrering samt utveckling av riskminimerande metoder under övergångsperioder. Senast 2028 ska en nationell metod för kartläggning av teknikskuld kopplat till cybersäkerhet vara etablerad, och senast 2029 ska minst 60 procent av verksamhetsutövare ha en tidsatt moderniseringsplan för de system som hindrar integrering av avancerad teknik.

Krav som överstiger tillgängliga stödresurser

För att hantera ökade och överlappande regelverkskrav på ett effektivt och likvärdigt sätt utan att hindra införande av avancerad teknik krävs automatiserade och gemensamma compliance-funktioner. För att åstadkomma detta ska NCSC i samarbete med berörda tillsynsmyndigheter:

- Tar fram krav och ger stöd för utveckling av automatiserade processer för kontinuerlig regelefterlevnad.
- Initiera utveckling och etablering av gemensamma verktyg som förenklar rapportering och uppföljning för verksamheter som omfattas av flera regelverk.

För att genomföra detta krävs investeringar i tekniska plattformar för efterlevnadskontroll, samordning för att undvika dubbelrapportering och stöd för integration med befintliga system. Detta inkluderar utveckling av en gemensam metod för att identifiera och prioritera teknik som inte är kompatibel med avancerad riskhanteringsteknik och som därmed hindrar införande av centrala cybersäkerhetsförmågor, samt stöd till verksamheter för att ta fram långsiktiga och samordnade moderniseringsplaner.

Omvärldsbevakning av policyforum, standarder, regelverk och teknikutveckling

För att nationella prioriteringar, vägledningar och regelverk ska vara aktuella, samordnade och baserade på internationell teknikutveckling behövs en samlad och systematisk omvärldsbevakning. För att åstadkomma detta ska NCSC (huvudansvar) med FRA, FMV, MCF och PTS i samverkan med SIS, TK 318:

- Inrätta en samlad nationell funktion för löpande teknik- och hotanalys.
- Publicera återkommande analyser och rekommendationer.
- Integrera omvärldsbevakningen i NCSC:s verktygslåda.
- Säkerställa att analyser och rekommendationer tas fram enligt fastställd periodicitet och följs upp avseende faktisk användning hos berörda myndigheter.

För att genomföra detta krävs tydlig ansvarsfördelning och samordningsansvar, analyskompetens, etablerade samarbetsformer och moderna insamlingsverktyg. Detta förutsätter även en tydlig koppling mellan internationellt standardiseringsarbete och nationella behov, så att svenska prioriteringar inom cybersäkerhetsteknik får genomslag i relevanta standarder och tekniska ramverk.

Svenskt deltagande i internationella teknikinitiativ

Aktivt deltagande i internationella initiativ, pilotprojekt och testbäddar är en förutsättning för att svenska behov och erfarenheter ska påverka standarder och snabbt kunna omsättas nationellt. För att öka svenskt deltagande i internationella teknikinitiativ ska NCSC (huvudansvar) med MCF, FMV, PTS, FOI och sektorsmyndigheter i samverkan med Regeringskansliet och SIS, TK 318:

- Utforma nationella pilotprojekt så att de kan kopplas till EU, Nato och andra internationella satsningar.
- Etablera gemensamma testmiljöer med tydligt syfte och tydlig styrning.
- Säkerställa systematisk återföring av resultat till nationella riktlinjer.

För att genomföra detta krävs en klargjord samordningsroll, finansiering, avtalsstöd och etablerade modeller för internationell informationsdelning.

Svenska standardiseringsinitiativ och nationell styrning för nya teknologier

För att säkerställa svenskt inflytande, samordnat deltagande och effektiv införlivning av internationella ramverk krävs nationell styrning och prioritering av standardiseringsarbete. För att uppnå detta ska NCSC:s standardiseringsgrupp (myndigheter med uppdrag att styra, rådge eller kontrollera säkerhet) i samverkan med SIS TK 318:

- Etablera övergripande strategiska mål för vilka områden och standarder där Sverige bör delta i standardiseringsarbetet.

För att genomföra detta behöver ansvariga utses för specifika uppgifter som återrapporterar till NCSC samt övriga intressenter. Därutöver behöver budget tilldelas för tid samt deltagande i internationella standardiseringssamarbeten.

Ökat regelverk och implementering av avancerad teknik

Ett ökat regelverk samt implementering av avancerad teknik ska kunna utvärderas så att det sker kontrollerat, säkert och på ett kostnadseffektivt sätt. Användning av internationella standarder för certifiering och revision möjliggör kontrollerad, säker och kostnadseffektiv implementering av regelverk och avancerad teknik. För

att uppnå detta ska tillsynsmyndigheter tillsammans med externa och interna revisioner:

- Säkerställa att de som behöver kompetens för implementering och revision av certifiering utifrån standarder utbildas. Genomförandet ska utgå från internationella standarder för revision såsom ISO 27006, ISO 27007, ISO 27008 samt standarder för certifiering av produkter och tjänster.

Verktygsstöd för compliance

Regelverk ställer teknikkrav men verksamheter saknar verktygsstöd för compliance. För att åtgärda detta ska NCSC (huvudansvar) med MCF och tillsynsmyndigheter:

- NCSC säkerställer att tydliga rekommendationer och listor över standardiserade funktioner för compliance ingår i verktygslådan.
- Verksamheter implementerar processer för loggning, spårbarhet och rapportering.

För att genomföra detta krävs en tydlig ansvarsfördelning, investeringar i tekniska plattformar och sektorsgemensam samordning.

Indikatorer

Referenser

Främja utbildning, forskning och ökad medvetenhet om cybersäkerhet

Enligt NIS 2-direktivets artikel 7.2 f) Riktlinjer för att främja och utveckla cybersäkerhetsutbildning, cybersäkerhetskompetens, medvetandehöjande åtgärder och forsknings- och utvecklingsinitiativ, samt vägledning om god praxis och kontroll för cyberhygien som riktar sig till medborgare, intressenter och entiteter.

Definitioner och begrepp

Cyberhygien: Ett sätt att se på cybersäkerhet som liknar personlig hygien. Det vill säga enkla och regelbundna rutiner som alla kan följa för att skydda sin data och sina enheter mot incidenter.

Inkubator: En organisation med syfte att främja och underlätta nystartade företags tillväxt och lönsamhet.

Innovationskontor: En servicefunktion vid lärosäte som syftar till att nyttiggöra den forskning som bedrivs.

Innovationsupphandling: En process som påbörjas när en offentlig verksamhet har identifierat ett behov som inte täcks av det utbud som finns på marknaden.

Science park: En mötesplats som samlar företag, universitet och högskolor samt offentlig sektor i syfte att driva innovation och utveckling.

Introduktion

För att kunna uppnå en tillfredställande cybersäkerhet i Sverige krävs kompetens och kunskap i hela samhället: hos privatpersoner, offentliga aktörer och hos näringsidkare. Förutom cybersäkerhetskompetensen hos specialistroller behöver den allmänna medvetenheten höjas hos individer och organisationer. Kompetensförsörjningen inom cybersäkerhet behöver därför stärkas i hela samhället genom insatser riktade mot allmänheten och civilsamhället, grundskola och gymnasium, yrkesutbildningar och fortbildning, högskole- och universitetsutbildningar samt till forskning och innovation.

Denna policy avser att täcka hela kompetensförsörjningsområdet inom cybersäkerhet, och är indelad i tre områden som motsvarar följande mål i den nationella strategin för cybersäkerhet: Mål 7: Ökad cybersäkerhetsmedvetenhet och cyberhygien i samhället, Mål 8: Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet, samt Mål 9: Stärkt forskning och innovation på cybersäkerhetsområdet. De tre målområdena behandlas nedan parallellt.

Avgränsning

Policyn är i huvudsak avgränsad till civil utbildning, forskning och ökad medvetenhet om cybersäkerhet i det svenska samhället och omfattar endast i begränsad omfattning internationella relationer, som exempelvis inom ramen för EU. Vidare omfattar policyn inte utbildning, forskning och ökad medvetenhet om cybersäkerhet inom försvarssektorn och internationella samarbeten inklusive Nato.

Nulägesbild

Ökad cybersäkerhetsmedvetenhet och cyberhygien i samhället

Samhällets motståndskraft mot kriser och hot är beroende av att Sveriges befolkning har en allmän cybersäkerhetkompetens. Samhällets digitalisering skapar möjligheter, men innebär också att risker och hot blir mer komplexa och svåröverskådliga. Cyberhot, informationspåverkan och störningar i kritisk infrastruktur ökar behovet av medvetandehöjande åtgärder och ökad kunskap om cyberhygien hos allmänheten.

ENISA Threat Landscape 2024 report lyfter incidenter som riktas mot det civila samhället och allmänheten genom social manipulering, dataläckor och påverkanskampanjer. Enisa konstaterar i rapporten ENISA 2024 State of Cybersecurity in the union att hälften av EU-medborgarna saknar den digitala kompetens som behövs för att fullt ut kunna delta i samhället, vilket hindrar deras tillgång till tjänster som tillhandahålls online. Undersökningar visar bland annat att olika sociodemografiska grupper har olika nivåer av digital kompetens och att medvetenheten är låg när det gäller cyberbrottslighet och vilka rapporteringsmekanismer som finns för allmänheten.

Sverige har en högre digital kompetens och ett högre deltagande i det digitala livet jämfört med genomsnittet i EU, i synnerhet i de yngre åldersgrupperna, och ligger över medel i EU vad gäller medborgares medvetenhet om god cyberhygien. I Sverige finns hos offentliga aktörer, privata företag, branschorganisationer och föreningar ett brett engagemang för att öka befolkningens kunskap och medvetenhet kring cybersäkerhet, och en stor vilja för samarbete mellan dessa parter. Sverige har även flera långsiktiga och etablerade insatser för kunskaps- och medvetandehöjning bland befolkningen och en god samverkan mellan myndigheter och medborgare.

Det finns i Sverige fortfarande ett gap mellan olika grupper i samhället, där ålder är den viktigaste faktorn men det finns även skillnader mellan stad och landsbygd. Sverige följer här EU-mönstret vad gäller klyftor i den digitala kompetensen. Det finns även stora grupper som är särskilt utsatta, exempelvis personer med

funktionshinder eller med migrationsbakgrund, vars behov av målgruppsanpassade insatser inte uppfylls och vars kunskaper inte når upp till genomsnittet.

Flera svenska undersökningar visar att medvetenheten om cyberbrott höjts och när det gäller risken att utsättas för digitala brott ökar oron. Utvecklingen mot ett säkrare beteende går dock långsamt och inte i takt med den digitala utvecklingen i samhället. Även i övriga EU har invånarnas tilltro till sin förmåga att skydda sig mot cyberbrott minskat, vilket tyder på att medvetenheten om cybersäkerhet sannolikt har ökat bland EU-medborgarna. Det saknas idag information riktad till allmänheten kring de mer långsiktiga konsekvenserna av incidenter i samhället, vilket gör det svårt för privatpersoner att se betydelsen av deras eget beteende i ett samhällsperspektiv. Informationen finns idag, men är anpassad till och kommuniceras endast med offentliga och privata aktörer.

Civilsamhället har en stark roll i det svenska samhället, där två av tre svenskar är engagerade i någon form av förening eller trossamfund Civilsamhället hanterar stora informationsmängder där känslig information kan ingå. Samtidigt faller civilsamhället inte under någon specifik lagstiftning, utöver GDPR. Kompetensen kring säker informationshantering varierar kraftigt och det har inträffat flera incidenter där känslig information gått förlorad eller hamnat i fel händer. Det finns idag möjlighet för civilsamhället att söka finansiellt stöd för att bedriva utbildning om cybersäkerhetsfrågor, men däri ingår inte möjligheten att ansöka om stöd för den egna föreningens eller trossamfundets cybersäkerhetsarbete eller att utbilda de egna medlemmarna. Det saknas även utbildningsmaterial att tillgå som riktar sig specifikt till civilsamhället och det finns ingen myndighet med stödjande funktion i cybersäkerhetsfrågor som civilsamhället kan vända sig till för hjälp.

Det finns många organisationer i offentlig sektor som arbetar med frågan, men inget formaliserat ansvar för allmänhetens kunskaps- och medvetandehöjning på cybersäkerhetsområdet. Allmänheten vet inte till vem de ska vända sig för att få hjälp och stöd i frågorna, och det finns inget uttalat ansvar för grupper med större behov och utmaningar.

Regeringen beslutade den 25 januari 2024 att ge Post- och telestyrelsen (PTS) i uppdrag (Fi2024/00172) att föreslå insatser för att öka andelen individer som är digitalt inkluderade, det vill säga individer som använder digitala tjänster. I resultatredovisningen av detta uppdrag gavs förslaget att PTS bör få ett utökat uppdrag att informera allmänheten om trygg och säker användning av internet, detta eftersom myndigheten ansåg det vara en vital del av arbetet med digital inkludering. PTS arbetar med allmänhetens digitalisering där säkerhet är en viktig del genom exempelvis initiativet Digitalidag som når cirka en miljon privatpersoner under en dag i oktober och telefontjänsten Ring Digitalidag där allmänheten kan ringa in med sina frågor. NCSC har idag uppgift att utveckla och

stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot och andra it-incidenter, med tydligt fokus på privata och offentliga aktörer. Samma fokus hade MSB och numera Myndigheten för civilt försvar i cybersäkerhetsfrågor, där kampanjen Tänk säkert var ett undantag då den vänder sig till allmänheten och små företag.

Tänk säkert-kampanjen

Fram till 2026 har Myndigheten för samhällsskydd och beredskap (MSB), Polismyndigheten och drygt 20 andra organisationer från privat sektor, offentlig sektor och föreningslivet gemensamt genomfört kampanjen Tänk säkert, för att öka medvetenheten och kunskapen om informationssäkerhet för allmänhet och små företag. Kampanjen stöttas av regeringen och har genom samarbeten nått ett brett genomslag i samhällets olika delar. Det finns utbildningar och informationsmaterial där besökare kan fortbilda sig året runt, den aktiva kommunikationen sker en månad om året.

Andra folkbildande initiativ

Utöver Tänk säkert genomförs även årliga informationssäkerhetsinsatser av andra aktörer. Ett exempel är kampanjen Svårlurad som är en gemensam kampanj från Sveriges banker. Ett annat är Digitalidag som samlar aktörer över hela Sverige och når runt en miljon människor under en dag i oktober varje år, med kunskapshöjande aktiviteter som höjer den digitala delaktigheten och säkerhetsmedvetenheten. Gemensamt för alla initiativen är att de sker i samverkan mellan flera olika parter, oftast från både offentlig och privat sektor.

Säkerhetskollen - ett initiativ från Stöldskyddsföreningen

Säkerhetskollen är en webbplats där invånare och företagare kan fortbilda sig inom cybersäkerhet, och som skickar ut varningar om pågående digitala brott. Stöldskyddsföreningen arbetar aktivt med polis, myndigheter, försäkringsbolag och banker för att ligga i framkant i kampen mot den digitala brottsligheten.

Internetstiftelsen

Internetstiftelsen tillhandahåller evenemang och utbildningsinsatser som gör det enklare att förstå och använda internets tjänster och som bidrar till ökad kompetens och digital säkerhet. Internetstiftelsen vänder sig till allmänheten, men särskilt till äldre och yngre. Bland annat har de utvecklat digitala lektioner som används i skolorna.

Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet

Företag i Sverige liksom i övriga Europa upplever stora svårigheter med att rekrytera lämpliga kandidater till lediga tjänster, och bristen på cybersäkerhetskompetens utgör ett väsentligt bekymmer. EU:s cybersäkerhetsbyrå,

Enisa, identifierar kompetensbristen som ett av de tio största hoten och en av framtidens stora utmaningar inom cybersäkerhet.

Det finns flera EU-initiativ som syftar till att främja kompetensförsörjning inom cybersäkerhet, bland annat kring det europeiska ramverket för cybersäkerhetskompetens, European cybersecurity skills framework (ECSF), och den europeiska kompetensakademin för cybersäkerhet, Cyber Skills Academy.

Kompetensbehovet i Sverige

I Sverige har ett antal olika undersökningar och analyser gjorts avseende kompetensförsörjning inom informations- och cybersäkerhetsområdet, med samstämmiga resultat: behovet av kompetens på området kommer att fortsätta öka samtidigt som svårigheterna att hitta personal som kan möta behoven redan idag är betydande. Det finns en könsobalans där kvinnor är väsentligt underrepresenterade på cybersäkerhetsrelaterade tjänster.

Cybersäkerhet som utbildnings- och yrkesområde har en tydligt teknisk framtoning, samtidigt som ämnet är relevant inom många andra områden som samhällsvetenskap och juridik, och i andra delar av en organisation som exempelvis inköp samt ledning och styrning.

Gemensamt för resultaten av gjorda undersökningar är också att de pekar på svårigheterna i att beräkna både arbetsmarknadens behov och utbildningsväsendets försörjning av relevant kompetens. En central utmaning är att kompetenser inom informations- och cybersäkerhet benämns på många olika sätt. Detta gäller dels i hur olika roller och förmågor beskrivs hos organisationerna på arbetsmarknaden, dels i hur utbildningsaktörer beskriver de färdigheter som ingår i olika utbildningsalternativ. Bilden blir än mer komplex genom att arbetet ofta är tvärfunktionellt och kräver en kombination av kompetenser från olika områden, samtidigt som behoven varierar beroende på verksamhetens art och vilka legala krav den omfattas av.

En annan problematik som lyfts är svårigheten för arbetssökande inom området att etablera sig på arbetsmarknaden. Kriterier för lediga tjänster är ofta högt ställda med krav på utbildning såväl som erfarenhet inom specifika teknologier eller höga förväntningar om att en person ska kunna täcka organisationens behov av cybersäkerhet när det gäller såväl teknik och styrning som juridik och kommunikation.

Utbildningsutbudet

Utbudet av utbildningar inom cybersäkerhetsområdet är relativt brett, både avseende innehåll, format och målgrupper. Såväl universitet och högskolor som yrkeshögskolor erbjuder längre utbildningsprogram samt kortare kurser. Kurserna ges dels inom ramen för andra program, exempelvis juridik, dels som fristående alternativ. Fristående kurser tillhandahålls även av kommersiella aktörer, och

fokuserar ofta på snabb kompetensutveckling för redan yrkesverksamma, för att matcha den snabba utvecklingen inom ämnesområdet.

Det finns också en stark utveckling av kommersiella certifieringar av individuell kompetens. I den flora av olika kurser och utbildningar som finns på området, där det kan vara svårt att värdera vilken kompetens de resulterar i, blir internationella certifieringar attraktiva som kompetensbenämningar både för arbetsgivare och för den som utbildar sig.

Samtidigt finns utmaningar med att kartlägga utbildningsutbudet inom området, även här delvis på grund av brist på enhetliga benämningar. En annan problematik kommer av att informations- och cybersäkerhet ofta erbjuds som valbara kurser eller inriktningar, men att det saknas samlad statistik över hur många som väljer dessa kurser eller hur många som examineras från sådana inriktningar.

Utöver formell utbildning finns en mängd andra möjligheter till kompetensutveckling inom cybersäkerhet, exempelvis genom nätverk, metodstöd, övningar och andra sätt att utveckla arbetet och sin egen kompetens.

Initiativ för ensning av benämningar

Komplexiteten i att kartlägga såväl kompetensbehovet på arbetsmarknaden som utbildningsutbudet gör det svårt att sammanställa en tydlig bild av var gapen faktiskt finns.

Flera undersökningar har prövat att tillämpa Enisas cybersecurity skills framework (ECSF) som ramverk för beskrivning av roller och kompetenser på cybersäkerhetsområdet, och mappa det till det svenska utbildningsutbudet. Ramverket täcker olika typer av roller med tekniska, juridiska och ledningsnära aspekter av cybersäkerhetsarbetet. Undersökningarna bedömer att ramverket är relevant och har en enkel struktur men kan behöva anpassas för svenska förhållanden för att fullt ut möta behoven från både arbetsmarknads- och utbildningssynpunkt. Bland annat efterfrågas koordinerande roller som informationssäkerhetssamordnare särskilt i Sverige.

Utbildning på lägre nivå

Inom grundskola och gymnasium har digital kompetens funnits med i läroplanen, där säkerhetsaspekter ingår men inte behandlats på ett enhetligt sätt. Vad som omfattas och hur det tas upp beror på lärarens och/eller skolans engagemang och kompetens.

De lärare och skolor som väljer att behandla ämnet gör det ofta med hjälp av material från andra aktörer. Flera organisationer tillhandahåller material som kan användas i skolan på olika nivåer, och/eller erbjuder aktiviteter och utbildning på fritiden för barn och ungdomar; bland annat Unga forskare, Kodcentrum,

Internetstiftelsen och Stöldskyddsföreningen. Olika typer av spelaktiviteter, hackatons och andra initiativ förekommer också, i syfte att öka intresset för ämnet.

Stärkt forskning och innovation på cybersäkerhetsområdet

I Sverige har det bedrivits forskning och innovation inom cybersäkerhet under lång tid, bland annat genom lärosäten som KTH, Chalmers, Linköping universitet och Stockholms universitet samt forskningsinstitut som RISE och FOI. Men det nationella ekosystemet är snabbt växande med flera nya aktörer och insatser som bidrar till kunskapsuppbyggnad, kommersialisering och tillämpning av cybersäkerhetslösningar. Bland de nyare nationella initiativen är en central aktör det nationella samordningscentret för forskning och innovation inom cybersäkerhet, NCC-SE som organiseras inom Myndigheten för civilt försvar, fram till 1 juli 2026 då funktionen flyttas till NCSC vid FRA. NCC-SE har i uppdrag att främja samarbete mellan forskningsinstitut, företag och offentlig sektor för att skapa bättre cybersäkerhetslösningar genom att knyta kontakter mellan svenska och europeiska forskare och företag, underlätta för svenska aktörer att svara på europeiska forsknings- och innovationsutlysningar, utforma och genomföra nationella utlysningar inom cybersäkerhet samt stödja EU:s kompetenscentrum för cybersäkerhet, ECCC, tillsammans med andra nationella samordningscenter.

Cybernoden är den nationella kompetensgemenskapen inom cybersäkerhet som Myndigheten för civilt försvar är ålagd att upprätta och samordna genom CCCN-förordningen.[145] Cybernoden leds och inriktas av Myndigheten för civilt försvar/NCC-SE men drivs på deras uppdrag av RISE och finansieras av Vinnova till och med 2026. Därefter tar FRA/NCSC över finansieringen av Cybernoden. Cybernodens primära syfte är att utgöra en samverkansplattform där aktörer med intresse för och behov av innovation och forskning inom cybersäkerhet kan mötas och samverka för ett gynnsammare innovationsklimat samt ökad svensk konkurrenskraft och export inom cybersäkerhet. Cybernoden är den största kompetensgemenskapen i Europa med över 420 medlemmar (december 2025) från privat, offentlig och idéburen sektor samt akademin.

Cybercampus Sverige är en statligt finansierad nationell satsning och ett samarbete mellan universitet, institut, myndigheter och företag i hela Sverige med uppdrag att stärka kompetensförsörjning, utbildning och forskning inom cybersäkerhet. Verksamheten ska möta behov som inte adresseras av någon av de andra aktörerna på cybersäkerhetsområdet, som stöd för alla samhällssektorer. KTH är huvudman för uppdraget att etablera och utveckla Cybercampus Sverige.

[145] Europaparlamentets och rådets förordning (EU) nr 887/2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum (EUT L 202, 8.6.2021, s. 1–34).

Tillsammans utgör NCC-SE, Cybernoden och Cybercampus centrala delar av den nationella infrastrukturen för stärkt forskning och innovation inom cybersäkerhet tillsammans med ett flertal regionala och lokala initiativ.

Forskning

Cybersäkerhetsforskning bedrivs inom många olika akademiska miljöer och på forskningsinstitut i Sverige. Det finns ingen aktuell översikt kring vilken typ av eller i vilken omfattning cybersäkerhetsforskning som bedrivs. Cybercampus sammanfattar läget som att cybersäkerhetsforskningen är konkurrenskraftig med starka forskargrupper men att den varken är välkoordinerad eller har något större tvärvetenskapligt fokus.[146] Även om cybersäkerhetsforskningen i Sverige inte framförallt bedrivs tvärvetenskapligt omfattar den både tekniska, organisatoriska och samhälleliga dimensioner av cybersäkerhet och säker digitalisering. Metoder för att skydda komplexa, sammankopplade system, säkerhet i industriella styrsystem och kommunikationsinfrastruktur samt möjligheter och hot kopplat till AI, automatisering och avancerad datahantering är några av delarna av den tekniska forskningen, liksom kryptografi, post-kvantkryptering, integritetsbevarande teknik och principer för säker mjukvaruhantering och arkitektur. Även forskning som inte har ett strikt tekniskt fokus genomförs, kring teman som människans roll i cybersäkerhet, riskhantering, informationssäkerhet, robusthet i samhällsviktiga verksamheter och cybersäkerhet inom teknologier med både civila och militära tillämpningsmöjligheter, så kallad dual-use. SIGS-CyberSec[147] är ett exempel på en svensk forskarskola inom cybersäkerhet. Forskarskolan består av ett konsortium av datavetenskaps- och informatikforskare från fyra svenska universitet: Corporate Research School vid Karlstads universitet, Blekinge tekniska högskola, Försvarshögskolan och Örebro universitet. SIGS-CyberSec är finansierad av KK-stiftelsen.

Det finansiella stödet till forskning är till stor del inriktad på långsiktigt kunskapsbyggande. Finansiering kommer i betydande grad från:

- Vetenskapsrådet, för grundläggande och tillämpad forskning
- Stiftelsen Strategisk Forskning
- Wallenbergstiftelserna och andra privata stiftelser
- KK-stiftelsen, ofta för tematiska och projektbaserade insatser
- EU:s forskningsinriktade delar av Horisont Europa, särskilt kluster 3, Civil säkerhet för samhället
- Vissa nationella myndigheter via riktade satsningar, exempelvis Myndigheten för civilt försvar
- Natofinansiering

[146] https://www.cybercampus.se/research, besökt 2025-12-04
[147] https://sola.kau.se/sigscybersec/

- EU-programmet DIGITAL kan även erbjuda finansiering till forskningsnära utvecklingsprojekt, särskilt om fokus är implementering av lösningar som baseras på forskningsresultat. På så sätt kompletterar DIGITAL Horisont genom att möjliggöra utveckling och vidarenyttjande av forskning i praktiska tillämpningar.

Innovation

Innovation inom cybersäkerhet handlar till stor del om utveckling, testning och införande av nya lösningar, tjänster och arbetssätt. Utöver de nationella satsningar som stöttar både forskning och innovation inom cybersäkerhet finns det flera andra initiativ med fokus på att stärka innovationskapacitet i både offentlig och privat sektor. En central aktör är den nationella cybersäkerhetsinnovationshubben Sweden Secure Tech Hub som hjälper små och medelstora techföretag att skapa säkrare digitala produkter och lösningar. Hubben är ett samarbete mellan sex svenska science parks. Finansieringen består av en kombination av EU-medel, nationella och regionala stödmedel samt de deltagande science parks egna insatser.

Utöver science parks, inkubatorer och liknande innovationsfrämjande verksamheter spelar lärosätenas innovationskontor en viktig roll genom stöd kring kommersialisering av forskningsresultat, immaterialrättsliga frågor samt stärkande av entreprenörskap genom bland annat stöd vid uppstart av företag och samverkansprojekt. På så sätt stärker de relationerna mellan akademi och privat och offentlig sektor samt bidrar till nyttiggörandet av forskningsresultat.

Många privata företag bedriver egen forskning och utveckling inom cybersäkerhet, både på egen hand och i samverkan med akademi eller andra aktörer. Deras innovationsarbete kan bidra till Sveriges stärkta förmåga på cybersäkerhetsområdet.

Finansiering av cybersäkerhetsinnovation syftar ofta till att främja utveckling, tillämpning och skalning av cybersäkerhetslösningar och kommer bland annat från:

- Vinnova, bland annat genom programmet Avancerad digitalisering
- Myndigheten för civilt försvar via NCC-SE genom nationella utlysningar och finansiellt stöd till tredje part (FSTP) riktat till små och medelstora företag
- Tillväxtverket och regionala utvecklingsaktörer
- EU-programmet DIGITAL för kapacitetsuppbyggnad och införande av cybersäkerhetsteknik
- De innovationsrelaterade delarna av Horisont Europa

Innovationsupphandling kan användas när en upphandlande organisation inom den offentliga förvaltningen har ett behov som inte kan lösas träffsäkert av

marknaden utan kräver utveckling eller forskning. Det finns idag begränsad statistik kring hur vanligt innovationsdrivande upphandling är i Sverige och heller inga siffror som specifikt handlar om cybersäkerhet. Innovationsupphandling skulle kunna användas som ett sätt att köpa nya, innovativa cybersäkerhetsprodukter eller cybersäkra tjänster och produkter och därigenom också stötta utvecklingen av dessa.

Analys av nuläget

Ökad cybersäkerhetsmedvetenhet och cyberhygien i samhället

Den ständigt accelererande tekniska utvecklingen medför alltmer svåröverskådliga hot och risker. Detta ökar behovet av att höja allmänhetens kunskap om cybersäkerhet. Det gäller inte minst bland barn och ungdomar, som är den framtida arbetskraften.

En befolkning med hög medvetenhet och stabila vanor inom cyberhygien är mer motståndskraftig mot cyberhot. Detta bidrar till en säkrare digital miljö för alla och möjliggör ett allmänt deltagande i den digitala tidsåldern samtidigt som det främjar ekonomisk tillväxt. Sveriges befolkning har ännu inte en tillräckligt hög medvetenhet och stabila vanor inom cyberhygien. Det innebär att individer själva, såväl som organisationerna där de är verksamma, är mer sårbara för cyberrisker än de hade behövt vara.

Det är visserligen positivt att Sverige ligger över genomsnittet i EU vad gäller digitalt deltagande, kunskap och medvetenhet, men deltagandet, den allmänna kunskapen och medvetenheten är trots det otillräcklig, i synnerhet hos vissa grupper. Möjliga orsaker till klyftorna mellan olika grupper kan vara språkhinder men även funktionshinder i form av hörselnedsättning, synsvårigheter och inlärningssvårigheter. Andra faktorer kan vara vid vilken tidpunkt i livet personen introducerades i det digitala livet, och i vilken samhällelig kontext personen befinner sig i såsom utbildningsnivå, bostadsort eller om personen har en anställning.

Dessa grupper är svåra att nå genom allmänhetsundersökningar, eftersom detta kräver förmåga att svara på undersökningar via telefon eller webb. Personer som exempelvis har läs- och talsvårigheter eller av andra skäl inte kan svara eller nås, kan därför inte anses fullt belysta i någon undersökning och nås troligen inte av medvetandehöjande insatser i lika hög grad trots att det hos dessa grupper finns stora behov. Bristen på kartläggning av grupper med särskilda behov, gör det svårt att minska klyftorna genom anpassade och riktade satsningar gentemot dessa grupper.

Klyftor mellan olika grupper när det gäller medvetenhet om cyberhygien kan leda till att vissa stängs ute från delar av samhället när tjänster går över till att bli enbart eller i stor utsträckning digitala, vilket både Internetstiftelsens och Enisas undersökningar pekar på. I slutändan kan detta påverka både människors livskvalitet och möjlighet att delta i vårt demokratiska samhälle.

Att både svenskar specifikt och EU-medborgare generellt uttrycker en större oro för att bli utsatta för cyberbrott än tidigare tyder dock på att medvetenheten om cyberrisker har ökat bland befolkningen, vilket bör innebära ökade förutsättningar för befolkningen att ta till sig vägledning och förbättra sin cyberhygien.

Arbetet med att höja allmänhetens kunskaper och medvetande kring cybersäkerhetsrisker försvåras av att det saknas formaliserade ansvar och uppdrag i samhället när det gäller målgruppen allmänheten. De initiativ som görs utgår oftast från organisationens egna insikter om behovet och punktinsatser, snarare än långsiktiga satsningar som täcker hela gruppen allmänheten. Vissa grupper i samhället täcks in av flera satsningar medan andra blir utan, och allmänheten vet inte vart de ska vända sig för stöd. Myndigheter som endast vid vissa tillfällen försöker nå allmänheten i dessa frågor når ofta inte hela vägen eftersom de saknar etablerade mötesplatser och sändningstid för sina budskap i dessa frågor.

Det är positivt att civilsamhället når brett i samhället och har ett ökat engagemang i cybersäkerhetsfrågor, troligen ett resultat av de incidenter som uppdagats som berör just civilsamhället. Det är dock problematiskt att det oftast saknas både resurser och inom cybersäkerhet i civilsamhället. Bristen på kunskaps- och finansiellt stöd från samhället leder till att endast stora, resursstarka civilsamhällesorganisationer har möjlighet att förbättra den egna och medlemmarnas cybersäkerhet. Näringslivet har en liknande position i samhället, där de engagemang som finns är positiva men skulle behöva och kunna täcka in fler företag för att på så sätt nå en större del av samhället. Det finns alltså en stor potential i näringslivet att bidra i förändringen genom ett bredare engagemang.

Sammantaget har Sverige flera positiva omständigheter som ett brett engagemang i frågorna, flera etablerade och effektiva initiativ och en kunskapsnivå hos befolkningen som är över genomsnittet i EU. Det kan dock också konstateras att vi även i Sverige behöver höja nivån ytterligare vad gäller cyberhygienen hos befolkningen i stort så att utvecklingen på säkerhetsområdet kan närma sig utvecklingen inom digitaliseringen och motsvara de krav som det säkerhetspolitiska läget ställer på samhället.

Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet

Det är positivt att frågan om kompetensförsörjning finns på dagordningen och uppmärksammas genom olika initiativ och undersökningar. EU-utveckling pågår i

flera spår på området. Aktörer från olika samhällssektorer är aktiva och redo att verka för förändring, vilket ger bra förutsättningar för gemensamma insatser med brett stöd.

Det är också en styrka att det finns ett stort och varierat utbildningsutbud från olika typer av aktörer vilket gör det möjligt för dem som vill att yrkesutbilda sig, fortbilda sig eller komplettera en annan utbildning. På så sätt kan kompetens tillföras arbetsmarknaden på olika sätt och på ett individuellt plan kan det ske i flera skeden av en yrkesbana. Det finns också goda möjligheter till kompetensutveckling på egen hand eller för en organisation genom utbudet av stöd som metodstöd, övningar och nätverk.

I fråga om kompetensförsörjning ligger den övergripande utmaningen i det faktum att samtidigt som efterfrågan på personer med cybersäkerhetskompetens ökar snabbt, växer också bristen på människor med rätt kompetens som kan fylla behoven. Detta leder till flera problem, bland annat att företag, myndigheter och andra organisationer får svårt att upprätthålla ett tillfredsställande arbete med cybersäkerhet, vilket gör dem mer sårbara för störningar i verksamheten som kan drabba både kunder/medborgare/användare och uppdragsgivare. En annan konsekvens är att arbetsmarknaden snedvrids då den eftertraktade kompetensen samlas hos de arbetsgivare som upplevs erbjuda de mest attraktiva villkoren, med följden att andra får än större svårigheter att rekrytera till kritiska roller.

Det finns en förbättringspotential i att länka samman utbildning med arbetsmarknad. Många arbetsgivare har svårigheter att identifiera vilken kompetens de behöver. Bristen på kontaktytor mellan arbetsgivare och arbetssökande i form av praktikplatser, liksom svårigheten i att formulera effektiva tjänstebeskrivningar som släpper in nyutexaminerade, leder till att arbetsgivare och arbetstagare i värsta fall inte hittar varandra. Den här typen av otydlighet och osäkerhet riskerar att minska områdets attraktionskraft. En annan aspekt är behovet av utbildning/fortbildning till redan yrkesverksamma, där arbetsgivare har möjlighet att effektivt bidra till kompetensförsörjningen.

Orsakerna till kompetensbristen finns på olika plan. Allt för få intresserar sig för ämnet, det uppfattas som tekniskt, svårt och abstrakt och många kommer främst i kontakt med det i samband med incidenter, vilket ofta väcker negativa associationer snarare än ett intresse för området som en möjlig yrkesväg. Säkerhetsaspekter tas inte konsekvent upp som en naturlig del av digital kompetens i skolundervisning eller i samhället i stort. Bristen på kvinnor inom området lämnar inte bara stora resurser outnyttjade för arbetsmarknaden, bristande jämställdhet leder också generellt till sämre resultat jämfört med mer heterogena arbetsgrupper.

Bilden av cybersäkerhet som karriärväg är otydlig och visar inte generellt sett på den tvärvetenskaplighet som ämnet inbegriper, vilket gör att potentiellt

intresserade personer missar möjligheten och arbetsmarknaden får ett mindre och smalare underlag.

En central svårighet med att främja och underlätta kompetensförsörjningen ligger i bristen på detaljerad information, om behoven och tillgången på kompetens samt hur mycket kompetens som kan tillföras genom utbildningar. Avsaknaden av gemensamma beskrivningar för roller och kompetenser inom cybersäkerhet, såväl ur arbetsgivar- som utbildarperspektiv, försvårar både matchning, jämförelser och behovsbedömningar. I kombination med en bristfällig helhetsbild av den utbildningskapacitet som finns blir det mycket svårt att avgöra om utbildning finns inom rätt kompetenser i förhållande till behoven. Detta i sin tur försvårar beslut om vilka åtgärder som behöver vidtas, och även utvärdering av resultaten.

Mot den bakgrunden är det positivt att ett ramverk utvecklats på EU-nivå som syftar till att etablera en gemensam benämningsstruktur för cybersäkerhetskompetens, och att det enligt genomförda studier förefaller användbart för svenska förhållanden.

Det finns idag olika initiativ som försöker råda bot på kompetensbristen, men orsaker såväl som potentiella lösningar spänner över aktörer i olika delar av samhället – olika myndigheter, utbildningssektorn, arbetsmarknaden – vilket ställer krav på samverkan som det inte finns förutsättningar för i dagsläget.

Vad gäller utbildning på lägre nivåer så leder dagens nivå av styrning till att elever inte har likvärdiga möjligheter att lära sig grundläggande cybersäkerhet. Otydligt ansvar och skillnader i intresse och kompetens resulterar i att vilken undervisning eleverna får på området i stor utsträckning beror på vilken skola man går på eller vilken lärare man har. Den påbörjade revideringen av läroplanen utgör dock en möjlighet, liksom de befintliga initiativ som finns på flera håll, inte minst från aktörer inom näringslivet och den ideella sektorn.

Stärkt forskning och innovation på cybersäkerhetsområdet

Det är positivt att det finns många aktörer och nätverk inom det nationella ekosystemet för forskning och innovation inom cybersäkerhet. Nationella initiativ som samlar aktörer från många sektorer underlättar både samverkan och bidrar till ökad förståelse för olika organisationers förmågor, behov, möjligheter och utmaningar. Science parks, inkubatorer och liknande innovationsfrämjande miljöer stöttar innovation inom cybersäkerhet och underlättar för aktörer att hitta rätt. Olika typer av finansiering skapar en dynamisk miljö där olika aktörer kan hitta ändamålsenlig finansiering för forskning och utveckling. Innovationskontor stöttar redan idag kommersialisering av relevanta forskningsresultat inom cybersäkerhet och bygger broar mellan akademi och näringsliv. Att innovationsupphandling används som verktyg underlättar för offentliga aktörer att skapa de lösningar som

främjar verksamheter och medborgare på bästa sätt samtidigt som forsknings- och innovationsinitiativ får medel till utveckling som kan bidra till tillväxt.

Det är negativt att de närliggande nationella initiativen gör det svårt för behovsägare att se deras respektive nyttor och hitta till det nätverk som skapar störst effekt. Otydligheten mellan initiativen skapar en osäkerhet hos målgrupperna. Konsekvenserna blir dubbelarbete för de nationella initiativen som måste guida målgrupperna rätt, dubbelarbete för målgrupperna som behöver läsa in sig på flera initiativ samt osäkerhet kring vem som gör vad med risk för att maximal nytta inte nås. Orsakerna är mångfacetterade men bottnar i de nationella initiativens uppdrag med stora och ibland oklara gränsytor, bristande koordinering mellan initiativen och bristande tydlighet i kommunikationen gentemot målgrupperna.

Det är negativt att bristande förmåga och resurser för koordinering och samverkan mellan science parks, inkubatorer, liknande innovationsfrämjande miljöer och de nationella initiativen skapar risk för att maximal nytta inte uppstår. Konsekvensen blir att de regionala och lokala satsningarna inte alltid kan guida målgrupperna rätt samtidigt som de nationella initiativen inte känner till de lokala och inte heller kan leda målgrupper rätt, att möjligheten att dra nytta av varandra och dela erfarenheter inte omhändertas och att samma arbete genomförs på olika ställen vilket inte är resurseffektivt. Orsakerna handlar framförallt om brist på resurser till omvärldsbevakning, nätverkande och kommunikation samt otydliga mandat.

Det är negativt att Sverige trots satsningar inom cybersäkerhet har få beviljade ansökningar inom EU:s stora finansieringsprogram Horisont Europa och DIGITAL i förhållande till sina europeiska grannländer. Intresset från svenska aktörer för att ansöka om EU-finansiering inom cybersäkerhet har hittills varit relativt lågt trots finansieringsbehov. Konsekvensen blir att Sverige minskar chansen till att trygga finansiering för forskning och innovation, bidra med och utveckla sin kunskap och kompetens på den internationella arenan och därigenom minska möjligheten för att vara ett framstående forsknings- och innovationsland och en ledande kunskapsnation inom cybersäkerhet. Orsakerna handlar framförallt om begränsad kunskap om finansieringsmöjligheterna, krav på egenfinansiering som är svåra för målgrupperna att möta, utmaningar kring att skriva träffsäkra ansökningar och svårigheter kring att skapa internationella konsortium på grund av bristande internationella nätverk.

Det är negativt att innovationskontor har begränsade möjligheter att stötta cybersäkerhetsinitiativ. Konsekvensen blir att chansen till kommersialisering av forskning från akademin gällande cybersäkerhet inte maximeras och möjligheten till nya, värdeskapande tjänster och produkter missas. Orsakerna handlar om den bristande tillgången på cybersäkerhetsexpertis och ovana att driva

kommersialisering av tvärvetenskapliga eller icke-tekniska forskningsresultat hos vissa aktörer.

Givet det stora behovet för både cybersäkerhetsprodukter och cybersäkra tjänster och produkter är det negativt att innovationsupphandling inte nyttjas i större utsträckning för att säkerställa inköp av ändamålsenliga tjänster och produkter. Konsekvensen blir att offentlig sektor inte får tillgång till ändamålsenliga cybersäkerhetslösningar och att leverantörer missar möjligheter till att utveckla och väsentligt förbättra cybersäkra produkter och tjänster. Orsaken till att detta inte sker beror på flera komplexa faktorer men hänger samman med offentliga aktörers begränsade resurser till innovativa inköp, osäkerhet i hur marknadsdialoger kan ske på ett korrekt sätt, låg kompetens kring innovationsdrivande upphandling och låg kompetens kring cybersäkerhet.

Målbild 2029

Ökad cybersäkerhetsmedvetenhet och cyberhygien i samhället

År 2029 har allmänhetens kunskap och medvetenhet om cybersäkerhet ökat till en nivå där människor använder samhällets digitala tjänster på ett säkerhetsmedvetet sätt. Förutsättningar finns för alla grupper i samhället att få och ta till sig målgruppsanpassad information och kunskap kring ett säkert beteende. Allmänheten kan få kunskap kring hybridhot och hur individers beteende påverkar samhället.

År 2029 finns en infrastruktur och ansvarsfördelning där aktörer med ansvar för cyberhygien och medvetenhet snabbt kan skapa nya medvetandehöjande insatser om cybersäkerhet och cyberhygien när det behövs, och effektivt nå målgrupper som särskilt behöver medvetandegöras. Infrastrukturen är känd i samhället, och privatpersoner, civilsamhälle och näringsliv vet var de kan få stöd och information.

År 2029 arbetar aktörer i alla delar i samhället med kunskaps- och medvetandehöjande insatser till sina respektive målgrupper. Civilsamhället och näringslivet har stöd och utbildningsmaterial att tillgå både för att arbeta med den egna organisationens cybersäkerhet och med individers. Deras arbete ger en bred täckning för medvetandehöjande insatser och når även de med särskilda behov.

Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet

År 2029 finns en etablerad samverkansstruktur mellan olika samhällsaktörer med syfte att främja kompetensförsörjning inom cybersäkerhetsområdet. Cybercampus har en ledande roll i arbetet, där även utbildningsaktörer och

arbetsmarknadsrepresentanter ingår tillsammans med NCSC, NCC-SE/Cybernoden och andra relevanta myndigheter.

År 2029 finns en enhetlig terminologi för kompetenser och roller inom cybersäkerhet som används av arbetsgivare och utbildningsaktörer vilket effektiviserar matchning på arbetsmarknaden. Statistik baserad på den enhetliga terminologin finns, som ger underlag för specifika insatser med syfte att stärka kompetensförsörjningen. Den underlättar också för utbildningsaktörer att anpassa utbildningsutbudet till arbetsmarknadens behov.

Arbetsgivare samverkar med utbildningsaktörer för att stärka kompetensförsörjningskedjan genom att erbjuda praktikplatser, instegsjobb, fortbildning och omskolningsmöjligheter, vilket bidrar till att relevant kompetens kommer arbetsmarknaden tillhanda.

År 2029 finns ett stort intresse för cybersäkerhet och studenter såväl som yrkesverksamma söker sig till utbildningar inom området, vilket bidrar till att minska kompetensbristen. Bilden av cybersäkerhetsområdet uppvisar en högre grad av tvärvetenskaplighet, vilket breddar perspektiv och tillämpningsområden samt bidrar till att nya grupper intresserar sig för ämnet. Kvinnor och andra underrepresenterade grupper uppmuntras att söka cybersäkerhetsutbildningar.

År 2029 är cybersäkerhet inkluderat i undervisningen inom grundskolan och gymnasiet, på ett sätt som är likvärdigt för alla elever oavsett skola, skolform, bostadsort. Detta bidrar till en stärkt medvetenhet i samhället i stort och ökar också möjligheterna att väcka intresse för cybersäkerhet som yrkesbana.

Stärkt forskning och innovation på cybersäkerhetsområdet

2029 är det svenska ekosystemet för stöttande av forskning och innovation inom cybersäkerhet fortsatt dynamiskt med äldre och nyare initiativ som bidrar till stärkt samverkan och kunskapsspridning. De nationella satsningarna NCC-SE, Cybernoden och Cybercampus koordinerar sina respektive uppdrag samt samarbetar nära varandra och synkar sin kommunikation för att säkerställa att det är lätt för målgrupperna att hitta rätt. De samlar forskare, behovsägare och nuvarande samt potentiella leverantörer av cybersäkerhetslösningar och cybersäkra produkter och tjänster och bidrar med både strategiska insikter och praktiskt och konkret stöd. De tre nationella initiativen har långsiktig finansiering vilket skapar goda förutsättningar för långsiktiga satsningar.

Till 2029 fortsätter science parks, inkubatorer och andra innovationsfrämjande aktörer spela en viktig roll i att skapa regionalt och lokalt engagemang för forskning och innovation inom cybersäkerhet. Genom SISP sker effektiva kontakter med de nationella initiativen och kommunikation flödar smidigt mellan

de olika aktörerna, vilket gör det lätt för behovsägare, leverantörer och entreprenörer att hitta rätt i ekosystemet. Utvecklingen underlättar för start-ups inom cybersäkerhetsområdet att etableras, växa och leverera tjänster och produkter. Till 2029 fortsätter också innovationskontor att stödja kommersialisering av forskningsresultat, skyddande av immaterialrättigheter och entreprenörskap inom cybersäkerhet. Genom stärkt samverkan mellan dem och de nationella samt regionala och lokala initiativen, bland annat genom SISP och SNITTS (nätverket för akademins innovationsfrämjare)[148], säkerställs att innovationskontoren får kontinuerlig uppdatering på utveckling inom cybersäkerhetsområdet, förenklad tillgång till cybersäkerhetskompetens, uppdateringar kring finansieringsmöjligheter och tillgång till information om möjligheter till konsortiumbygge. Dessa insatser leder till att ett ökat antal forskningsresultat kommersialiseras och kommer marknaden till nytta samt att fler företag inom cybersäkerhetsområdet med grund i akademin lanseras.

2029 finns fortfarande många nationella finansieringsmöjligheter för forskare inom cybersäkerhet. Finansieringen till tvärvetenskaplig forskning har uppmuntrat forskare från olika discipliner att samverka samtidigt som den ämnesbundna forskningsfinansieringen fortsatt underlättat djupare specifik forskning. NCC-SE har i utökad grad bidragit med både generellt och individualiserat stöd till aktörer att söka medel genom EU-program som Horisont och DIGITAL. De nationella initiativen har tillsammans med relevanta aktörer bidragit till att underlätta ekonomiskt stöd till medfinansiering vilket gjort det väsentligt lättare för intressenter att ansöka till utlysningarna. Ett stadigt ökande antal aktörer har sökt och fortsätter söka både EU- och andra internationella medel. Sverige är fortsatt aktiva i att påverka innehåll i arbetsprogram för kommande utlysningar i ett tidigt skede genom samverkan mellan bland annat de nationella initiativen och regeringskansliet.

2029 används innovationsdrivande upphandling i ökad omfattning för att säkerställa att offentlig sektor får tillgång till ändamålsenliga cybersäkerhetsprodukter samt cybersäkra produkter och tjänster. Upphandlingsmyndigheten och NCSC har fått i gemensamt uppdrag att sprida information om innovationsupphandling för cybersäkerhet och därigenom nått ut till både köpande och säljande sida. Cybernoden, NCC-SE och Cybercampus anordnar regelbundet rundabordssamtal, utställningar eller andra arenor där offentliga behovsägare och leverantörer kan föra dialog och utforska möjligheter.

[148] https://www.snitts.se/

Åtgärder för att uppnå målbilden

Ökad cybersäkerhetsmedvetenhet och cyberhygien i samhället

1. Allmänhetens kunskap och medvetenhet om cybersäkerhet och hybridhot ökas genom
   a. År 2027 införs en årlig nationell mätning kring svenskars kunskap och medvetenhet inom cybersäkerhet och hybridaktiviteter där det även finns utvärderingsfrågor om genomförda insatser.
   b. Formaliserad samverkan upprättas under 2026 mellan olika myndigheter för att motstå hybridaktiviteter, där säkerhet går hand i hand med kunskap om medier och information samt desinformationskampanjer. I samverkan bör MPF, NCSC, PTS och Mediemyndigheten ingå.
   c. Myndigheter ansvariga för Tänk säkert-kampanjen får ett större uppdrag att arbeta under hela året och inte bara under oktober. Kampanjen får tydligare uppdrag att arbeta spetsigare och mer anpassat till vissa målgrupper. Civilsamhället bjuds in att delta i medvetandehöjande kampanjer som Tänk säkert.
   d. NCSC får i uppdrag att kontinuerligt ta fram och kommunicera exempel på långsiktiga konsekvenser av cyberincidenter, både för samhället och individen, anpassat till målgruppen allmänheten.
2. Insatser inom cybersäkerhet och cyberhygien når bredare och effektivare i samhället genom att
   a. En formaliserad samverkansstruktur tas fram där statliga myndigheter, ideella organisationer och företag bedriver informations- och utbildningsinsatser inom cybersäkerhet för allmänheten.
   b. PTS uppdrag kring digital inkludering utökas till att innefatta säkerhet. PTS får det övergripande ansvaret för arbetet med medvetandehöjande insatser gentemot allmänheten och arbetar i samverkan med andra aktörer. Aktörer som NCSC och Myndigheten för civilt försvar bör ingå men kan även innefatta andra relevanta aktörer som exempelvis Internetstiftelsen och Stöldskyddsföreningen.
   c. Samverkande aktörer skapar målgruppsanpassade aktiviteter och utbildningsmaterial för särskilt utsatta grupper. PTS ansvarar för behovskartläggning och samordning av aktiviteter.
3. Fler aktörer som arbetar med kunskaps och medvetandehöjande insatser inom cybersäkerhet uppnås genom att
   a. Näringsliv och civilsamhälle uppmanas att i högre grad arbeta med att kunskaps- och medvetandehöjande insatser till sina respektive målgrupper.

b. MUCF får i uppdrag att ge stöd och fördela medel till civilsamhällesorganisationer som vill främja digital kompetens och säkerhetsmedvetande inom organisationen och hos organisationens medlemmar.
c. Samverkande myndigheter får i uppdrag att ta fram informations- och utbildningsmaterial som aktörer inom näringsliv och civilsamhälle kan tillgå för att kunna genomföra kompetenshöjande aktiviteter om cyberhygien i sina respektive verksamheter.

Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet

1. Senast 2027 får Cybercampus ett utpekat ansvar att stödja och utveckla samverkansstruktur mellan olika samhällsaktörer i syfte att främja kompetensförsörjningen på nationell nivå. Till 2028 har regeringen utrett och säkerställt långsiktig finansiering av ansvarsuppdraget (Se även **Fel! Hittar inte referenskälla.**).
2.
    a. Cybercampus får i uppdrag att leda utveckling av en enhetlig terminologi för kompetenser och roller inom cybersäkerhet, baserad på European Cybersercurity Skills Framework (ECSF). Arbetet sker i samverkan med NCSC samt representanter för arbetsgivare och utbildningsaktörer. I uppdraget ingår också att marknadsföra terminologin och ta fram stöd för tillämpning hos arbetsgivare och utbildningsaktörer. Vidare ingår att föra dialog med relevanta myndigheter för att underlätta användningen av terminologin för officiell statistik.
    b. Relevanta myndigheter (såsom SCB, UKÄ, Arbetsförmedlingen) får i uppdrag att utreda hur terminologin kan införlivas med befintliga ramverk för utbildnings- och arbetsmarknadsstatistik, om möjligt följt av uppdrag för genomförande.
    c. Relevant myndighet (såsom Cybercampus) får i uppdrag att sammanställa och publicera statistik över arbetsmarknadens behov respektive utbildningssektorns tillgång på cybersäkerhetskompetens baserat på den enhetliga terminologin.
3. Cybercampus och NCSC/NCC-SE genom Cybernoden får i uppdrag att bidra med samordning och stöd till arbetsgivare och utbildningsaktörer för att underlätta kopplingar mellan utbildning och arbetsmarknad för studenter under och efter utbildning.
4.
    a. NCSC får i uppdrag att arbeta tillsammans med andra aktörer inom området för att stärka och bredda bilden av cybersäkerhet som yrkesområde.
    b. Utredning av finansiellt stöd till aktörer som

- arbetar med utveckling och spridning av stödmaterial och aktiviteter som belyser cybersäkerhet ur ett bredare perspektiv, med fokus på exempelvis beteendevetenskapliga, juridiska och organisatoriska aspekter.
- verkar för att förbättra representationen av olika grupper i cybersäkerhetsrelaterade utbildningar och yrken.

5.
   a. Senast 2027 får Skolverket i uppdrag att förtydliga ansvar och lärandemål i relevanta styrdokument, samt samordna och utveckla befintliga initiativ och resurser, i syfte att ensa undervisningen. NCSC stödjer med sakkunskap.
   b. Under 2027 får Skolverket i uppdrag att ta fram stöd och fortbildning för lärare avseende cybersäkerhet. NCSC stödjer med sakkunskap.

Stärkt forskning och innovation på cybersäkerhetsområdet

1. Under 2026 etableras en formaliserad samverkan mellan NCC-SE, Cybernoden och Cybercampus för en tydligare roll- och ansvarsfördelning. Detta kommuniceras till berörda målgrupper. Till 2028 har regeringen utrett hur långsiktig finansiering av initiativen kan säkras och säkerställt att huvudmännen har specifik finansiering till dem.
2. Med början 2026 sker formell samverkan mellan NCC-SE, Cybernoden, Cybercampus och SISP där de nationella initiativen är sammanhållande/inbjudande med fokus att dela kunskap, erfarenheter och nätverk för att underlätta för start-ups och SMF:er att utveckla och sälja cybersäkerhetstjänster och -produkter. Även SNITTS bjuds in till kontinuerlig dialog för att säkerställa relevant informationsdelning med det innovationsstöttande systemet inom akademin.
3. Från 2026 har NCC-SE vidareutvecklat och behovsanpassat sina erbjudanden vad gäller direkt stöd till aktörer med intresse för att delta i EU-utlysningar. Under 2026 har regeringen, i den mån behov finns, utrett möjligheter för medfinansiering till internationella forsknings- och innovationsprojekt samt hittat möjliga vägar och distributörer av sådan medfinansiering. Senast 2027 finns möjlighet att ansökan om sådan finansiering. Från 2026 och framåt ökar Sverige sitt aktiva arbete för att påverka innehåll i arbetsprogram för kommande utlysningar. NCC-SE utreder hur och säkerställer att man i utökad utsträckning uppmuntrar aktörer att delta på konsortiumbyggande evenemang samt finansierar aktörernas resekostnader.
4. Regeringen ger senast 2027 NCSC och Upphandlingsmyndigheten i uppdrag att tillsammans utreda om behov finns av att vidareutveckla det stöd som Upphandlingsmyndigheten idag erbjuder inom innovationsupphandling till att även innehålla specifik information kring

innovationsdrivande upphandling inom cybersäkerhetsområdet. Om utredningen visar att behov finns ska utvecklingen av detta påbörjas senast 2028. Vid samma tid ökar Cybernoden, NCC-SE och Cybercampus sitt fokus på temat och erbjuder sina målgrupper möjligheter att utöka sin kunskap inom det.

Indikatorer

Referenser

Stärkt informationsdelning på cybersäkerhetsområdet

Enligt NIS 2-direktivets artikel 7.2 h) Riktlinjer, inbegripet relevanta förfaranden och lämpliga verktyg för informationsutbyte för att stödja ett frivilligt informationsutbyte om cybersäkerhet mellan entiteter i enlighet med unionsrätten.

Definitioner och begrepp

Frivillig informationsdelning: Delning som sker utanför lagstadgade rapporteringskrav.

Hotindikator (IOC): Tekniskt spår som kan tyda på intrång/skadlig aktivitet (till exempel IP, domän, hash).

Informationsdelningsarrangemang: Organiserad form för frivillig delning (forum, nätverk, ISAC eller plattform) med gemensamma regler för deltagande och hantering.

Interoperabilitet: Förmåga att utbyta och använda information mellan system/aktörer utan specialanpassning.

Lagstiftning: Nationell och internationell lag eller förordning som är tillämpbar på området frivillig informationsdelning.

Lagstyrd informationsdelning: Informationsdelning som sker utifrån lagstadgade rapporteringskrav (till exempel CSL).

Långsiktig informationsdelning (NIS 2 artikel 29.1 b): Delning som stärker cybersäkerhet över tid (till exempel lärdomar, metoder, trender).

Nationell lägesbild: Sammanställd och löpande uppdaterad bild av hot, sårbarheter och incidenter.

Operativ informationsdelning (NIS 2 artikel 29.1 a): Delning för att snabbt förebygga, upptäcka eller hantera pågående incidenter (till exempel varningar och indikatorer).

Organisation: Organisationer i vidare bemärkelse, inkluderat både verksamhetsutövare och organisationer som inte per definition omfattas av detta begrepp

Standardiserad säkerhetskontaktpunkt: Publicerad (i till exempel security.txt) och uppdaterad kontaktväg för säkerhetsärenden (sårbarheter/incidenter).

Taxonomi: Klassificering/terminologi för att beskriva information på ett jämförbart sätt.

Verksamhetsutövare: Myndigheter, kommuner, regioner, privata företag och andra organisationer som omfattas av NIS 2.

Introduktion

Informationsdelning och samarbete mellan organisationer är avgörande för samhällets och verksamheters förmåga att förebygga, upptäcka och hantera cyberhot och incidenter. I artikel 29 i NIS 2-direktivet kan två huvudsakliga inriktningar för informationsdelning urskiljas:

1. Operativt inriktad delning som syftar till att snabbt förebygga, upptäcka och hantera pågående incidenter, där effektiva standardiserade säkerhetskontaktpunkter och outreach-förmåga är centrala;
2. Långsiktigt inriktad delning som stärker den generella cybersäkerhetsnivån genom ökad medvetenhet, delning av hotindikatorer och sårbarheter, metodutveckling och samarbete mellan offentliga och privata aktörer.

Informationsdelning sker dels enligt lagstadgade rapporteringskrav, dels frivilligt genom nätverk, forum och tekniska plattformar för säker informationsöverföring. NIS 2-direktivet anger att frivillig informationsdelning mellan väsentliga och viktiga entiteter samt relevanta leverantörer ska främjas, samtidigt som deltagande eller utträde ur sådana arrangemang ska anmälas till behörig myndighet. Tillit mellan aktörer och gemensamma principer för hur information ska hanteras och delas är en grundläggande förutsättning för att informationsutbyte ska fungera.

Lagstadgade krav på informationsdelning och cybersäkerhet skärps genom den nya cybersäkerhetslagen (CSL), som genomför NIS 2-direktivet i svensk rätt och trädde i kraft den 15 januari 2026. Lagen innehåller uttryckliga krav på informationsdelning, bland annat genom CERT-SE och den gemensamma kontaktpunktens ansvar för att ta emot och vidareförmedla incidentinformation, samt som en integrerad del av det nationella cyberkrishanteringssystem som ska etableras. Parallellt införs Lagen om motståndskraft hos kritiska verksamhetsutövare (LMV), som genomför CER-direktivet och förväntas träda i kraft under 2026.[149]

Den föreslagna policyn för stärkt informationsdelning på cybersäkerhetsområdet har tagits fram av Myndigheten för civilt försvar och Försvarets radioanstalt (FRA), med bistånd av Försvarets materielverk (FMV), Försvarsmakten, Polismyndigheten, Post- och telestyrelsen (PTS) och Säkerhetspolisen.

[149] Sedan den 1 december 2025 har regelverket i Sverige förändrats i syfte att möjliggöra ökad informationsdelning mellan myndigheter. Sekretesshinder mellan myndigheter har i detta avseende undanröjts, vilket innebär att frivillig informationsdelning ligger i linje med den nationella utvecklingen för förbättrad samverkan och informationsutbyte. https://www.regeringen.se/pressmeddelanden/2025/12/nu-rivs-sekretessen-mellan-alla-myndigheter-i-sverige/

Avgränsning

Policyområdet inbegriper relevanta förfaranden och lämpliga verktyg för att stödja ett frivilligt informationsutbyte om cybersäkerhet mellan entiteter i enlighet med unionsrätten. Lagstyrd informationsdelning behandlas endast i den utsträckning som krävs för att ge kontext och tydliggöra den frivilliga delningens funktion och mervärde.

I första hand avses frivillig informationsdelning på nationell nivå mellan statliga myndigheter, regioner, kommuner och privata organisationer – både inom och mellan dessa kategorier.

På internationell nivå avses frivillig informationsdelning främst mellan svenska organisationer i andra länder, till exempel branschkollegor, genom internationella nätverk, samt frivillig informationsdelning kopplad till sekundära källor och mottagare på EU-nivå (exempelvis i CSIRTs Network och EU-CyCLONe).

Policyområdet omfattar både frivillig informationsdelning med omedelbart operativt syfte (artikel 29.1a i NIS 2) samt informationsdelning som syftar till att stärka den generella cybersäkerheten över tid (artikel 29.1b i NIS 2).

Nulägesbild

I Sverige sker omfattande frivillig informationsdelning på cybersäkerhetsområdet både nationellt och i internationella sammanhang, mellan offentliga, privata och idéburna aktörer, samt inom akademin. Det saknas en samlande struktur och plattform på nationell nivå, men det finns många olika initiativ med varierande fokus, syfte och deltagare. Organisationer har stor möjlighet att välja bland nätverk och fora.

Organisering av informationsdelningsmöjligheter

Nationella fora och nätverk

På nationell nivå finns flera etablerade nätverk för informations- och cybersäkerhet, både för offentliga aktörer, privat-offentlig samverkan (POS) och exklusivt för privata aktörer eller branschrepresentanter.

Inom den offentliga sektorn finns bland andra *Statligt nätverk för informationssäkerhet (SNITS)* som samordnas och leds av Myndigheten för civilt försvar, *Kommunernas Informationssäkerhetsnätverk (KIS)* som drivs ideellt av kommunrepresentanter och stöds av Sveriges Kommuner och Regioner (SKR), *Hälso- och sjukvårdens informationssäkerhetsnätverk (HoSIS)* som drivs av medlemmarna själva, *eSams expert- samt sakområdesgrupp Säkerhet*, samt *Dela digitalt* som om är en plattform där anställda kan dela både frågor och information. För samverkan rörande NIS 2 finns *NIS samarbetsforum* och *NIS tillsynssamordning* för sektorsansvariga tillsynsmyndigheter, vilka båda samordnas av Myndigheten för civilt försvar.

Cybernoden, Sveriges nationella kompetensgemenskap för forskning, innovation och kompetensförsörjning inom cybersäkerhet, är landets största nationella plattform för POS inom området som inriktas av NCC-SE hos Myndigheten för civilt försvar och drivs av RISE. Därutöver finns strukturerade former för POS inom flera samhällsviktiga sektorer, till exempel *Finansiella Sektorns Privat-Offentliga Samverkan (FSPOS)*, *BT POS Transportsektorn*, *Nationella Telesamverkansgruppen (NTSG)*, samt *Säkerhets- och försvarsföretagens (SOFF:s) cyberförsvarsgrupp*, som också driver en MISP-instans, *SOFF MISP*. *NIS privat-offentligt samverkansform (NIS POS)* är en plattform för dialog och erfarenhetsutbyte mellan tillsynsmyndigheter och branschorganisationer.

Bland branschspecifika fora finns bland andra *Forum för informationsdelning (FIDI)*, till exempel *FIDI-Drift* och *FIDI-SCADA* inom säkerhet i industriella informations- och styrsystem, samt genom NCSC:s sektorforum för finans och energi.

Inom akademin finns bland andra *Swedish IT Security Network for PhD Students (SWITS)*, *Forum for Cyber Security and Cyber Operations*, och *Sveriges universitet och högskolors it-chefs forum (ITCF)*.

Det finns också många nätverk och gemenskaper om cybersäkerhet som samlar branschkollegor, yrkespersoner och andra intresserade, varav vissa har medlemsavgifter. Några exempel är *Altingets cybersäkerhetsnätverk*, utbildningsföretaget *JUC:s nätverk i cybersäkerhet*, Svenska Försäkringsföreningens *Nätverk Informationssäkerhet i försäkringsbranschen* och *Svenskt CERT-forum*.

Internationella fora och nätverk

På internationell nivå finns branschfora för it-säkerhetsteam, exempelvis *Forum of Incident Response and Security Teams (FIRST)*, och *Task Force CSIRT (TF-CSIRT)*. Informationen som delas i forumen och nätverken används för informationsdelning nationellt, för förmågeutveckling, i utveckling av nya tjänster, och tillhandahållandet av stöd.

Det finns även EU-relaterade fora och nätverk där Sverige deltar med centrala myndigheter och innehållet kommer svenska organisationer till del i andra hand. Några är:

- *NIS Samarbetsgrupp* med syfte att samordna arbetet med att genomföra och tillämpa NIS 2. Nationella myndigheter från medlemsländer, EU-kommissionen och Enisa deltar.
- *Europeiska gruppen för cybersäkerhetscertifiering*, en expertgrupp som samordnar EU:s ramverk för cybersäkerhetscertifiering enligt Cybersecurity Act. Nationella certifieringsmyndigheter, EU-kommissionen och Enisa deltar.

- *Computer Security Incident Response Teaams Network (CSIRT-nätverket),* är ett operativt samarbetsnätverk där nationella CSIRT:er, CERT-EU och Enisa deltar.
- *European Cyber Crisis Liaison Organisation Network (EU-CyCLONe)*, är ett EU-nätverk för cyberkrishantering på strategisk nivå där nationella myndigheter för cyberkrishantering, EU-kommissionen, Enisa och CSIRT-nätverket deltar.

Tekniska stöd för informationsdelning

Inom befintliga nätverk och fora används idag mejlinglistor, kommersiella chattverktyg och samarbetsverktyg för att utbyta information mellan fysiska möten. Myndigheten för civilt försvars lägesbildssändningar över videolänk, CERT-SE:s blixtmeddelanden och veckobrev, samt information som Stöldskyddsföreningen delar inom ramen för *Säkerhetskollen* och *Digitala varningsgruppen* är några exempel.

Från offentlig sektor erbjuds *MISP-SE* som är en nationell plattform där svenska verksamhetsutövare kan dela och ta emot hotinformation. Delningen sker via verktyget *Malware Information Sharing Platform (MISP)* som används för att samla in, lagra, analysera och dela information om cyberhot och incidenter. MISP stödjer strukturerad och standardiserad delning av hotindikatorer (IOC), till exempel IP-adresser, domäner och skadlig kod. MISP kan hantera både manuell och automatiserad delning. CERT-SE förvaltar MISP-SE.

WIS är en portal för Sveriges civila beredskap där aktörer delar information före, under och efter samhällsstörningar. WIS innehåller funktioner som underlättar samverkan och samordning, bland annat stöd för att begära in och analysera information till en samlad lägesbild. Dokument, bilder, kartor eller annan information kan delas mellan aktörer eller inom den egna organisationen. Myndigheter, kommuner, regioner, frivilligorganisationer och privata aktörer med en roll i Sveriges civila beredskap får använda WIS.

Automatiska Notifieringar av Tekniska Sårbarheter (ANTS) är en informationsdelningstjänst som varnar anslutna organisationer när information upptäcks om tekniska företeelser som kan behöva åtgärdas, till exempel om enheter anslutit till övertagna botnät, om servrar har sårbara mjukvaror eller tjänster har sårbara konfigurationer. ANTS är kostnadsfritt och tillgängligt för alla svenska organisationer, både i offentlig och privat sektor, som vill ha hjälp med övervakning av sina angreppsytor på internet. Den svenska staten har full rådighet över vilka organisationer som ansluts till ANTS och vilka datakällor som används.

Det finns även informations- och varningstjänster som tillhandahålls av privata företag.

Organisationers förutsättningar

Många organisationer saknar kännedom om möjligheter till frivillig informationsdelning, tid för att delta i relevanta nätverk, samt förmåga att både agera på mottagen information och själva bidra med information.

Erfarenheter från EU och internationellt visar att organisationers benägenhet att dela cybersäkerhetsinformation påverkas av en kombination av juridiska, organisatoriska och tekniska förutsättningar. Osäkerhet kring rättsliga konsekvenser, till exempel risken för tillsyn eller sanktioner, kan göra att organisationer avstår från att dela information.

Studier från Enisa pekar på att bristande tillit, otydliga och svårtolkade regler, samt avsaknad av tydliga incitament är centrala hinder för informationsdelning i både lagstyrda och frivilliga arrangemang. [150]

Forskning om små och medelstora företag visar på begränsade resurser och brist på kompetens. Användbarhetsproblem och oro för hur känslig och affärskritisk information hanteras försvårar användningen av hotinformationsdelningstjänster, till exempel plattformar som MISP.[151]

Svenska mätningar som Cybersäkerhetskollen bekräftar att många offentliga organisationer saknar grundläggande förmåga att arbeta systematiskt med cybersäkerhet, vilket i praktiken begränsar deras kapacitet att både ta del av och bidra till frivillig informationsdelning. [152]

Analys av nuläget

Den svenska samverkanskulturen märks tydligt i arbetet med informationsdelning. Den stora mängden svenska fora och nätverk där cybersäkerhet diskuteras på olika nivåer, och data och erfarenheter delas indikerar en vilja och utgör en god grund för frivillig informationsdelning.

Brister som behöver adresseras består bland annat av:

1. Att Sverige inte har en tillräckligt samlad och träffsäker ordning för att få rätt cybersäkerhetsinformation till rätt aktör i rätt tid, i en form som går att agera på. Utmaningarna handlar dels om att roller och ansvar för vem som

[150] Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches December 2015 https://www.enisa.europa.eu/publications/cybersecurity-information-sharing
[151] Challenges to Small and Medium Businesses for Cyber Threat Intelligence Sharing, Mohamed Rifa, 2024 https://www.diva-portal.org/smash/get/diva2%3A1866623/FULLTEXT01.pdf
[152] Resultatredovisning av Cybersäkerhetskollen 2024 – Det systematiska cybersäkerhetsarbetet i den offentliga förvaltningen av MSB. https://rib.msb.se/filer/pdf/30971.pdf

ska dela vilken typ av information, med vilka mottagare och i vilken form, är otydligt fördelade, dels om att många verksamhetsutövare saknar tydliga och uppdaterade kontaktvägar för säkerhetsrelaterade ärenden. En bakomliggande orsak är att ingen aktör har eller har haft i uppdrag att presentera en helhetsbild över dessa frågor.

2. Att inte tillräckligt många organisationer nyttjar de nätverk och tjänster som finns. Bakomliggande orsaker är bland annat bristande kännedom om nätverk och tjänster, begränsningar hos dessa, resursbrist och omedvetenhet om varför det är viktigt.
3. Att det saknas samverkan mellan cybersäkerhetsområdet och aktörer som hanterar andra typer samhällskriser och civilt försvar, vilket innebär sämre förutsättningar att hantera kriser som har cyberrelaterade orsaker. En bakomliggande orsak kan vara att informationsdelning på cybersäkerhetsområdet framförallt rör tekniska förhållanden som är mest relevanta för cybersäkerhetsspecialister. Det bidrar till att cybersäkerhetsområdet avskärmas från den bredare krisberedskapen och det civila försvaret och att det inte byggs förmåga att samverka mellan cybersäkerhetsprofessionen och andra professioner med incident- eller krishanterande roller i det civila försvaret.
4. Att vissa tjänster och infrastrukturer ännu saknar funktionalitet som behövs för att möjliggöra och effektivisera informationsdelning, särskilt för många-till-många-delning. Bakomliggande orsaker är en komplex blandning av rättsliga utmaningar, höga kostnader och behov av prioritering av begränsade resurser hos aktörer som har nyckelroller i att tillhandahålla och utveckla sådana tjänster.
5. Att mikro-, små- och medelstora företag (SMF) samt idéburna aktörer endast i begränsad utsträckning kan försörjas med viktig cybersäkerhets-information. Bakomliggande orsaker är dels att det, med några undantag, saknas tjänster som är utformade efter sådana organisationers förutsättningar vad gäller kunskapsnivå, resurser och tid, dels att dessa organisationer har begränsade möjligheter att nyttja de tjänster som erbjuds.
6. Att det finns en oro för att dra till sig uppmärksamhet och tillsyn som kan hämma organisationers vilja att dela problem. Bakomliggande orsaker kan vara otydlighet och bristande kännedom om skyldigheter och grunder för tillsyn.
7. Att det finns en oro för att bryta mot lagen eller andra regelverk som gör att vissa avstår från att dela information. Bakomliggande orsaker kan vara att det saknas enkel tillgång till en tydlig beskrivning av rättsläget för den aktuella delningen, eller att det faktiska rättsläget inte medger enkel delning. Exempel på sådana rättsområden är hur GDPR, sekretess, dataskydd och konkurrensrätt påverkar frivillig informationsdelning.

Målbild 2029

Organisering av informationsdelningsmöjligheter

Nationell samverkansstruktur för frivillig informationsdelning

År 2029 har Sverige ett samordnat och sektorsöverskridande ekosystem för frivillig informationsdelning på cybersäkerhetsområdet. Statliga myndigheter, regioner, kommuner och privata organisationer deltar aktivt i informationsdelning på strategisk, operativ och taktisk nivå genom en bred flora av fora, nätverk och informationsnav som är bevarade och vidareutvecklade.

En nationellt förankrad samverkansstruktur säkerställer att aktörer har en gemensam förståelse för helheten, sin roll och sitt ansvar, samt tillämpar gemensamma principer för delning av information om hot, sårbarheter, incidenter och erfarenheter.

Inom denna struktur utgör NCSC en central nod för nationell samordning och stöd. Genom sin samverkans- och delningsstruktur möjliggör NCSC informationsutbyte på olika nivåer – från bred spridning av kunskap och lägesbilder till fördjupad dialog och långsiktig samverkan med utvalda aktörer. Den närmare utformningen av dessa nivåer utvecklas inom ramen för NCSC:s uppdrag.

Minst 80 procent av verksamhetsutövare som omfattas av CSL är registrerade för att ta del av NCSC:s nationella kunskap, lägesbilder och rekommendationer genom riktat informationsutbyte.

Fora och nätverk sprider och kontextualiserar varningar mellan aktörer och sektorsvisa aktiviteter inom minst 12 av de sektorer som definieras i NIS 2-direktivet bidrar med kvalitativa sektorsspecifika insikter, vilket stärker den samlade lägesbilden och förmågan att vidta relevanta åtgärder.

Långsiktiga och förtroendebaserade samverkansformer mellan centrala aktörer i det nationella ekosystemet har etablerats eller vidareutvecklats, i syfte att gemensamt stärka analysförmåga, metodutveckling och erfarenhetsutbyte.

Minst tio av de sektorer som omfattas av CSL har ett sektorsspecifikt forum/nätverk/informationsdelningsarrangemang som tillämpar en gemensam uppsättning nationella rekommendationer för frivillig informationsdelning i linje med NIS 2 artikel 29 och Enisas ISAC-inriktning. Arrangemangen har tydliga deltagarvillkor, roller, återkopplingsrutiner och hantering av konfidentialitet, till exempel TLP, vilket möjliggör ett förtroendefullt och skalbart informationsutbyte inom och mellan sektorer.

De etablerade informationsdelningsarrangemangen uppvisar en grundläggande och återkommande informationsdelning, och en majoritet har utvecklat strukturerad tvåvägsdelning med etablerade rutiner för analys, återkoppling och gemensamt lärande, i enlighet med en nationell mognadsmodell för informationsdelning, inspirerad av Nederländernas ISAC-vägledning. [153]

Informationsdelningsförmåga inom civilt försvar

År 2029 är cybersäkerhetsrelaterad informationsdelning integrerad i den bredare krisberedskapen och det civila försvaret. Integrationen utgår från löpande informationsdelning i vardagen mellan myndigheter, kommuner, regioner, företag, och civilsamhälle, och kan vid behov skalas upp och formaliseras för att stärka den gemensamma lägesbilden vid kris och höjd beredskap.

Informationsdelning mellan cybersäkerhetsområdet och krishanteringsområdet fungerar sammanhängande över tid och bidrar till att cyberrelaterade händelser hanteras som en integrerad del av samhällets samlade krisberedskap.

Rutinmässiga övningar genomförs årligen där både it-incidenthantering och cyberkrishantering ingår, och där frivillig informationsdelning via den nationella portalen och NCSC är en integrerad del av övningsscenariot. Övningarna bygger på vardagliga arbetssätt och informationsflöden och syftar till att öva – och i senare skede pröva – informationsdelning mellan cybersäkerhetsområdet och krishanteringsområdet. I övningarna deltar aktörer från beredskapssektorerna samt, där relevant, andra organisationer för att säkerställa att cybersäkerhetsarbetet är integrerat i det civila försvaret.[154]

Ansvarsfördelning och roller inom frivillig informationsdelning på cybersäkerhets-området följer ansvarsprincipen, vilket gör att förväntningarna på informationsdelning vid kris och krig är tydliga.[155]

Tekniska stöd för informationsdelning

Nationell cyberportal som stödjer säker och effektiv informationsdelning

År 2029 erbjuder staten en dedikerad, sektorsövergripande tjänst med tillhörande infrastruktur som möjliggör cybersäkerhetsrelaterad informationsdelning mellan

[153] Mognadsmodellen följer ett vedertaget mognadsresonemang men är framtagen av Nederländska NCSC/Digital Trust Center specifikt för ISAC-verksamhet. https://www.digitaltrustcenter.nl/sites/default/files/bestanden/website/NCSC%20Handreiking%20ISAC.pdfr

[154] Ansvariga myndigheter för olika samhällsviktiga funktioner och beredskapssektorer framgår av uppräkning på MCFs hemsida: https://www.mcf.se/sv/amnesomraden/beredskap-for-kris-och-krig/beredskapssystemet/det-civila-beredskapssystemet/

[155] Ansvarsprincipen innebär att den som i normala fall ansvarar för en verksamhet, till exempel en statlig myndighet eller kommun, också har detta ansvar under en krissituation. I Regeringens skrivelse 2024/25:121 Nationell strategi för cybersäkerhet 20 s. 5 poängteras särskilt att ansvarsprincipen ska gälla även för cybersäkerhetsområdet.

organisationer i Sverige, samt när så är relevant med strukturer på EU- och Natonivå. Tjänsten, i form av en nationell portal, stödjer både lagstyrda processer och frivillig informationsdelning och erbjuder en gemensam ingång till det samlade utbudet av cybersäkerhetstjänster och plattformar.

Verksamhetsutövare kan anmäla sig, genomföra reglerad rapportering, ta del av information och begära det stöd som de enligt CSL har rätt till samt bidra med frivillig information till myndigheter och andra organisationer. Det tekniska stödet bidrar direkt till en kontinuerligt uppdaterad och delad lägesbild.

Alla relevanta målgrupper, oavsett storlek eller organisatoriska förutsättningar, kan både bidra med information och ta emot information på ett säkert och praktiskt användbart sätt. Både befintliga och nya informationsdelningsarrangemang använder tjänsten som tekniskt stöd för säker informationsdelning.

I bakgrunden hanterar portalen den reglerade informationsdelningen inom EU, genom koppling till Enisas system för till exempel rapportering av gränsöverskridande sårbarhetsärenden eller incidenter.

Standardiserade säkerhetskontaktpunkter gör det lätt att hitta en tydlig kontakt för cybersäkerhetsrelaterade ärenden hos svenska organisationer. Användare av den nationella portalen kan hitta varandra i denna. Därutöver gör en bred användning av och kännedom om security.txt[156] att även allmänheten i Sverige och utomlands enkelt hittar rätt kontakt.

Organisationers förutsättningar

Kunskap, kapacitet och resurser att delta i informationsdelning

År 2029 har en stor andel svenska organisationer, inklusive sådana som inte träffas direkt av CSL, tillräcklig kunskap, kapacitet och resurser för att delta i informationsdelning på ett ändamålsenligt sätt. De förstår sin roll i ekosystemet och bidrar aktivt till Sveriges samlade cybersäkerhet. Den frivilliga informationsdelningen når därmed betydligt fler aktörer än enbart dem som genom lagkrav får kännedom om möjligheter att dela frivillig information.

Mikro-, SMF samt idéburna aktörer har kännedom om möjligheter till frivillig informationsdelning, förstår hur de kan delta och har kapacitet att både ta emot information och bidra med information. De nås av relevant och begriplig cybersäkerhetsinformation på en nivå som gör att den kan omsättas i konkreta åtgärder i den egna verksamheten.

Organisationers ledningar och styrelser, även i organisationer som inte träffas av CSL har tillräcklig förståelse för cyberrisker och informationsdelningens betydelse

[156] RFC 9116 https://www.ietf.org/rfc/rfc9116.pdf

för verksamhetens riskhantering, och tar ett aktivt ansvar för att säkerställa deltagande i relevanta informationsdelningsstrukturer.

Tydliga juridiska ramar gör det enkelt att dela information

År 2029 råder ett tryggt och förutsägbart delningsklimat för frivillig informationsdelning inom cybersäkerhetsområdet. Tydliga, samordnade och praktiskt tillämpbara juridiska ramar gör att verksamhetsutövare vågar dela relevant information utan att osäkerhet kring ansvar, sanktioner eller andra rättsliga risker, utgör att väsentligt hinder.

År 2029 har organisationer en gemensam och praktiskt användbar förståelse för hur lagstiftning som GDPR, säkerhetsskyddslagstiftningen och offentlighets- och sekretesslagstiftningen ska tillämpas vid frivillig informationsdelning.

Det är tydligt vilken information som kan delas, under vilka förutsättningar och i vilken form. Det finns vägledning med konkreta exempel, ett tydligt stöd för hantering av anonymisering, mallar och rutiner samt processer för delning av lärdomar. Särskild vägledning och exempel finns för bedömning av när information utgör personuppgifter och hur personuppgiftsbehandling kan undvikas eller minimeras.

Minst 75 procent av verksamhetsutövare uppger att de juridiska förutsättningarna för frivillig informationsdelning är tydliga och tillräckliga för att möjliggöra aktivt deltagande. Juridisk osäkerhet utgör inte längre ett väsentligt hinder för informationsdelning. Detta tar sig uttryck i att organisationer inte bara delar anonymiserad information, utan också – när det är nödvändigt vid allmänfarliga incidenter – delar icke-anonym information på ett kontrollerat och rättssäkert sätt, utan rädsla för oproportionerliga rättsliga konsekvenser.

År 2029 används anonymisering och pseudonymisering som förstahandsåtgärder vid delning av incidenter och lärdomar när detta är möjligt utan att informationsvärdet går förlorat. Samtidigt finns etablerade och rättssäkra processer för att dela icke-anonym information när det krävs vid allmänfarliga incidenter.

Kännedom om, användning av och återkoppling om nationella stöd

År 2029 har verksamhetsutövare som omfattas av CSL god kännedom om de nationella stöden på cybersäkerhetsområdet.

Minst 80 procent vet var de hittar vägledning för att ställa krav på cybersäkerhet i upphandlingar (upphandlingsstödet eller motsvarande), hur de kan ta del av nationell rådgivning (Cybersäkerhetsrådgivningen eller motsvarande) samt hur de lämnar strukturerad återkoppling om behov av kompletteringar till stödmaterial avseende frivillig informationsdelning.

Verksamhetsutövare som omfattas av CSL använder de nationella stöden i praktiken och återkommande mätningar av cybersäkerhetsmognad och systematiskt arbete med krav- och leveranskedjefrågor är etablerade delar av deras riskhantering. Minst 70 procent av verksamhetsutövarna genomför och rapporterar in Cybersäkerhetskollen (eller motsvarande) årligen.

Det finns en etablerad och aktiv återkopplingskultur där verksamhetsutövare och stödjande funktioner lämnar strukturerad återkoppling om identifierade krav- och vägledningsgap som leder till regelbundna förbättringar och uppdateringar av stödmaterial. Minst 300 inkomna, kategoriserade förbättringsförslag per år hanteras, och minst 50 procent av dessa omsätts i publicerade uppdateringar av stödmaterial inom fastställd förvaltningscykel.

Åtgärder för att uppnå målbilden

Organisering av informationsdelningsmöjligheter

Nationell samverkansstruktur för frivillig informationsdelning

1. Senast år 2027 ska NCSC publicera en beskrivning av en nationell samverkansstruktur för frivillig informationsdelning. Beskrivningen ska publiceras på nationell webbplats och/eller i den nationella portalen, och omfatta samtliga identifierade nationella informationsdelningsarrangemang. NCSC ska äga och förvalta denna beskrivning och säkerställa att den hålls uppdaterad.

2. Från och med år 2027 ska NCSC använda en fastställd och dokumenterad samverkansmodell och tjänstekatalog för analys, prioritering, planering och genomförande av samverkansinsatser. Det ska finnas en samlad och tydlig redovisning av vilka former av tjänster, informationsutbyten och stöd som erbjuds olika målgrupper inom det nationella ekosystemet.

3. Under perioden 2026–2029 ska NCSC successivt fördjupa sina samverkansinsatser från bred informationsspridning till att utveckla förmåga för mer strukturerade och återkommande samarbetsformer, såsom fora och sektorsvisa utvecklingsaktiviteter. Antalet strukturerade tvåvägsaktiviteter, såsom dialogmöten, gemensamma analyser och övningar, ska öka årligen, och senast 2029 ska minst 12 sektorer delta i återkommande fördjupad samverkan.

4. Senast 2029 ska minst 10 långsiktiga och återkommande samverkansrelationer med strategiskt viktiga offentliga och privata aktörer vara etablerade eller vidareutvecklade, i syfte att stärka gemensam analysförmåga, metodutveckling och erfarenhetsutbyte.

5. Från och med 2027 ska NCSC etablera nationella rekommendationer och ett nationellt stödprogram för frivilliga informationsdelningsarrangemang (ISAC-

liknande fora och nätverk) i linje med NIS 2 artikel 29 och Enisas ISAC-principer. Stödet ska omfatta:

a) vägledning och mallar som verkar förtroendebyggande, avseende deltagarvillkor, roller, konfidentialitet/TLP och återkoppling,
b) en nationell mognadstrappa med nivåer och kriterier (inspirerad av Nederländernas ISAC-vägledning),[157]
c) stöd för standardiserade arbetssätt och, där det är relevant, standardiserade informationsformat,
d) minst 5 utbildnings- eller vägledningsinsatser per år riktade till arrangemangens koordinatorer och nyckelroller, där genomförandet ska säkerställas genom tilldelning av tillräckliga personella resurser

Informationsdelningsförmåga inom civilt försvar

1. Under perioden 2026–2028 ska NCSC genomföra återkommande sektorsvisa och tvärsektoriella övningar som omfattar både it-incidenthantering och cyberkrishantering, där frivillig informationsdelning och återkoppling via nationella plattformar testas och utvärderas.

Övningarna ska genomföras under kris och krigsliknande former, bygga på de informationsflöden och arbetssätt som används i vardagen och utformas så att de kopplar samman cybersäkerhetsområdet med det bredare krishanteringsområdet och det civila försvaret. Syftet är att både träna aktörer och successivt pröva förmågan att dela, ta emot och använda cybersäkerhetsinformation som en integrerad del av samhällets krisberedskap.

2. NCSC ska i den nationella cyberkrishanteringsplanen, som NCSC för närvarande reviderar och avser att bygga ut efter verksamhetsövergången under 2026, tydliggöra ansvarsfördelning och tillämpningen av ansvarsprincipen och likhetsprincipen med beaktande av artikel 9 i NIS 2. Planen ska ange vilka aktörer som leder, samordnar och beslutar om informationsdelning vid cyberrelaterade kriser inom civilt försvar, samt beskriva roller, beslutsflöden, kommunikationskanaler, kriterier för frivillig informationsdelning, eskaleringsrutiner och samverkansmekanismer.

Tekniska stöd för informationsdelning

Nationell cyberportal som stödjer säker och effektiv informationsdelning

1. Under perioden 2026–2028 ska NCSC utveckla en nationell portal som stödjer

[157] Mognadsmodellen följer ett vedertaget mognadsresonemang men är framtagen av Nederländska NCSC/Digital Trust Center specifikt för ISAC-verksamhet. https://www.digitaltrustcenter.nl/sites/default/files/bestanden/website/NCSC%20Handreiking%20ISAC.pdf

processer för både lagstyrd och frivillig informationsdelning i större grupper av organisationer och många-till-många-delning. En gemensam ingång till hela utbudet av tjänster, målgruppsanpassade kanaler och en hög grad av automatisering ska förenkla informationsdelning för anslutna organisationer oavsett storlek och förutsättningar. Portalen ska minst kunna hantera teknisk hot- och incidentinformation (till exempel IOC:er och sårbarheter) läges- och varnings-information, erfarenheter och ”lessons learned”[158], samt stödjande material. Över tid ska portalen etableras som en central mötesplats för informationsdelning i cybersäkerhetsfrågor för organisationer i Sverige, oavsett om organisationen omfattas av CSL eller inte.

Åtgärder ska stegvis vidtas för att säkerställa att portalen har följande kapacitet följande år:

a) År 2026 påbörjas det grundläggande arbetet med att möjliggöra anmälan av verksamhetsutövare enligt kraven i både CSL och LMV, samt anmälan till tjänsten ANTS. Vidare så ska även begäran om stöd som verksamhetsutövare har rätt till enligt CSL kunna hanteras samt stödtjänster som Cybersäkerhetsrådgivningen finnas i portalen. Det ska också tas fram automatiserad rapportdistribution som går att nyttja till flera mottagare och som kan utfärda varningar.
b) År 2027 ska portalen utvecklas till att ha kapacitet så att alla tjänster i portalen nås med samma användarkonto. Det ska integreras ett säkert chatbaserat informationsutbyte, metodstödet för cybersäkerhet och Cybersäkerhetskollen. Det ska även utvecklas målgruppsanpassade kanaler för dels SMF, och dels företagsledningar, styrelser, och incident- eller krishanterande roller i det civila försvaret.
c) År 2028 ska portalen utvecklas ytterligare och kommande åtgärder består av att skapa förmåga för att kunna hantera standardiserade dataformat och taxonomier samt interoperabilitet med EU-nivåns plattformar.

2. Senast år 2028 ska NCSC förvalta en gemensam svensk profil för informationsdelning (format, taxonomier, TLP/principer och miniminivåer) som är synkad med EU/Enisa och versionshanteras. Med “miniminivåer” avses miniminivåer för (1) obligatoriska metadatafält vid delning, (2) informationsklassning och hantering (till exempel TLP-märkning), (3) validering och kvalitet (till exempel spårbarhet till källa och maskinläsbarhet), samt (4) åtkomststyrning och loggning i delningskanaler. Profilen ska vara styrande för den nationella portalen och rekommenderad för sektorsvisa forum och ISAC:ar.

3. Senast år 2028 ska NCSC också säkerställa att den nationella portalen stödjer samordnad delgivning av sårbarheter i enlighet med NIS 2 och

[158] ”Lessons learned” är en metod för att ta lärdom från incidenter där inblandade parter går genom incidenten, vad som gick bra, vad som gick mindre bra och vad som kan förbättras. Konkreta åtgärdspunkter tas fram

cyberresiliensförordningen, inklusive rutiner för rapportering till EU- och Natonivå.

4. NCSC ska införa krav på verifiering av standardiserade kontaktuppgifter vid anslutning, samt återkommande uppdaterings- och verifieringsrutiner, till exempel årlig omverifiering, automatiska påminnelser och tydlig roll/ansvar i portalen.

Organisationers förutsättningar

Kunskap, kapacitet och resurser att delta i informationsdelning

1. Senast år 2027 ska NCSC utveckla och etablera återkommande, riktade utbildnings- och vägledningsinsatser till mikroföretag och SMF om informationsdelningens betydelse för organisationers riskhantering, samt hur dessa aktörer praktiskt kan delta i relevanta informationsdelningskanaler.

2. Senast år 2027 ska NCSC utveckla och etablera återkommande, riktade utbildnings- och vägledningsinsatser till styrelser och ledningsgrupper om informationsdelningens roll i organisationers riskhantering och styrning, samt hur ledningen kan säkerställa att verksamheten deltar i relevanta informationsdelningsstrukturer. (Ytterligare utbildningsbehov för ledning specificeras i policy f).

Tydliga juridiska ramar gör det enkelt att dela information

1. Senast år 2027 ska NCSC ta fram och publicera en nationell regelverkskompass som beskriver samtliga aktuella lagkrav som kan beröras vid frivillig informationsdelning. För att underlätta för organisationer ska osäkerhet kring rättsliga hinder förtydligas. Kompassen ska bland annat innehålla specifik vägledning som hjälper organisationer i att förstå vad som faller under definitionen personuppgift enligt GDPR i samband med frivillig informationsdelning och ge tydliga exempel på vilken information som kan delas utan hinder i lagstiftning.

2. NCSC ska äga och förvalta regelverkskompassen och säkerställa att den hålls uppdaterad och utformad så att det blir så enkelt som möjligt för organisationer att våga dela information. NCSC ska bland annat sträva efter att minimera de processer där personuppgiftsbehandling är nödvändig, exempelvis genom anonymisering eller pseudonymisering som standard vid delning av information.

3. Senast år 2028 ska NCSC etablera och implementera en nationell process för att ta emot, bedöma och dela incidenter och lärdomar, inklusive hur anonymisering eller pseudonymisering ska hanteras när det är möjligt. Anonymiserade lärdomar ska publiceras i dedikerade plattformskanaler. När det krävs för att hantera eller förebygga en allmänfarlig nödsituation, och i dialog med berörd aktör, ska det finnas rättssäkra rutiner för att dela icke-anonym information.

4. Organisationer ska uppmuntras att själva dela erfarenheter i plattformen genom standardiserade mallar och vägledning och genom goda exempel som lyfts fram.

Kännedom om, användning av och återkoppling om nationella stöd

1. NCSC och berörda centrala aktörer ska under perioden 2026–2028 genomföra återkommande riktade outreach-insatser som säkerställer att minst 80 procent av verksamhetsutövare som omfattas av CSL känner till (1) upphandlingsstödet (eller motsvarande), (2) Cybersäkerhetsrådgivningen (eller motsvarande), samt (3) hur man lämnar återkoppling om behov av kompletteringar till stödets förvaltningsorganisation.

2. NCSC och berörda centrala aktörer ska år 2027 etablera och förvalta en standardiserad återkopplingskanal, till exempel via den nationella portalen, där verksamhetsutövare och stödjande funktioner (till exempel Cybersäkerhetsrådgivningen) kan rapportera identifierade krav- och vägledningsgap samt förslag på kompletteringar till stödmaterial.

Indikatorer

Referenser

Ökad cyberresiliens och cyberhygien hos små och medelstora företag

Enligt NIS 2-direktivets artikel 7.2 i) Riktlinjer som stärker cyberresiliensen och cyberhygienen hos små och medelstora företag, särskilt de som inte omfattas av detta direktiv, genom att tillhandahålla lättillgänglig vägledning och stöd för deras specifika behov.

Definitioner och begrepp

Cyberhygien: Ett sätt att se på cybersäkerhet som liknar personlig hygien. Det vill säga enkla och regelbundna rutiner som alla kan följa för att skydda sin data och sina enheter mot incidenter.[159] Cyberhygien kan ses som de förebyggande säkerhetsåtgärderna.

Cyberresiliens: En organisations förmåga att återhämta sig från incidenter. Detta innebär att säkerhetsåtgärder och krav ska finnas i hela infrastrukturen och livscykeln av produkter och tjänster i enlighet med riskaptit och regulatoriska krav, såsom de i EU:s cyberresiliensförordning (CRA).

Små och medelstora företag (SMF): Företag som sysselsätter färre än 250 personer och vars årsomsättning inte överstiger 50 miljoner euro eller vars balansomslutning inte överstiger 43 miljoner euro per år.[160]

Introduktion

Små och medelstora företag (SMF) utgör en betydande del av Sveriges ekonomi. Enligt Svenskt Näringsliv är 99,9 procent av företag i Sverige just SMF:er, de sysselsätter 64 procent av alla som är anställda i privat sektor och står för omkring 60 procent av omsättningen i näringslivet. Därigenom spelar SMF:ers förmåga att skydda affärshemligheter och deras generella motståndskraft en väsentlig roll i att skydda Sveriges samlade konkurrens- och motståndskraft. Små och medelstora företag finns inom alla branscher men omsättningen är störst inom tillverkning, handel, tjänster samt information- och kommunikationsteknik. Även om stora företag lämnar fler anbud i offentliga upphandlingar lämnas tre av fyra vinnande anbud av just små och medelstora företag. SMF:er är också ofta underleverantörer till stora företag som levererar till offentlig verksamhet. Tillväxtverkets statistik visar att ungefär 44 procent av de små och medelstora företagen har utvecklat och

[159] https://www.enisa.europa.eu/topics/cyber-hygiene
[160] https://www.vinnova.se/globalassets/huvudsajt/sok-finansiering/regler-och-villkor/dokument/engelska/eu-definition-smf.pdf

sålt nya eller väsentligt förbättrade produkter de senaste tre åren[161], något som visar på deras centrala roll som pådrivare av innovation.

Små och medelstora företag beskrivs som särskilt utsatta för incidenter då de saknar resurser både för förebyggande arbete och incidenthantering. När de drabbas av incidenter kan det leda till produktionsbortfall, störningar i samhällsviktiga tjänster och ekonomiska konsekvenser. Det är viktigt att SMF tar med sig allriskperspektivet i arbetet med cybersäkerhet, något som blev tydligt under covid-19 pandemin när det visade sig viktigt för alla att nyttja de digitala arbetssätten[162].

Avgränsning

Utgångspunkten i denna policy är att små och medelstora företag är företag med under 250 anställda vilket gör att även mikroföretag ingår. Policyn gör ingen väsentlig skillnad på SMF beroende på förkunskaper inom cybersäkerhet utan utgår främst från behov kopplade till företag där cybersäkerhet inte är främsta expertisområde.

Nulägesbild

Cyberresiliens och cyberhygien hos små och medelstora företag

Cyberresiliens innebär förmågan att kunna återhämta sig ifrån cybersäkerhetsincidenter. Cyberhygien är åtgärder som skyddar oss från cyberhot. Många små och medelstora företag har utmaningar rörande cyberresiliens och cyberhygien. År 2020 utsattes 80 procent av svenska bolag för minst en incident.[163] Cyberangreppsmetoder som förekommer är bland andra nätfiske, lösenordsattacker och angrepp via tredjepartsleverantörer. Det nationella cybersäkerhetscentret (NCSC) betonar att många företag saknar grundläggande skyddsmekanismer som incidenthantering och uppdaterade säkerhetspolicyer.[164] Tillväxtverket har lyft att det finns en utbredd medvetenhet om att cyberangrepp kan få stora konsekvenser för så väl ekonomi som förtroende, men att många företag trots detta inte har strukturerade processer eller kontinuitetsplanering.[165]

[161] https://tillvaxtverket.se/tillvaxtverket/statistikochanalys/statistikomforetag/foretagande/innovationsformaga.1609.html
[162] https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Cybersecurity%20guide%20for%20SMEs-online-single_page.pdf
[163] https://tillvaxtverket.se/download/18.6855bfcf184896002ffc18/1668765886578/S%C3%A4ker%20digitalisering%20i%20sm%C3%A5%20och%20medelstora%20f%C3%B6retag.pdf s27
[164] https://www.ncsc.se/siteassets/publikationer/cybersakerhet-i-sverige-2024.pdf
[165] https://tillvaxtverket.se/download/18.6855bfcf184896002ffc18/1668765886578/S%C3%A4ker%20digitalisering%20i%20sm%C3%A5%20och%20medelstora%20f%C3%B6retag.pdf

Samtidigt visar Myndigheten för civilt försvars årsrapport för it-incidentrapporteringen 2024 att cirka hälften av alla it-incidenter orsakades av misstag eller systemfel. Det tyder på att många organisationer saknar etablerade arbetssätt för ändringshantering.[166] Många incidenterna hade sannolikt kunnat förebyggas med hjälp av etablerade och inövade arbetssätt. När arbetssätt för ändringshantering saknas ökar risken för allvarliga incidenter och störningar. I Myndigheten för civilt försvars temarapport, ”Ändringar som både hotar och skyddar” från 2022, presenterar flera exempel på utmaningarna och dess konsekvenser.[167]

Rapporten ”Svenskt säkerhetsindex” listar ledningsförmåga som det viktigaste fokusområdet. Rapporten visar att en högre andel SMF:er än stora företag lutar sig på certifieringar som en strategi för tredjepartshantering vilket kan ses som ett tecken på att interna säkerhetsprocesser saknas. Enligt Myndigheten för civilt försvars metodstöd för systematiskt informationsarbete saknas ofta tydlig ansvarsfördelning, roller och rutiner för uppföljning.

En ytterligare omvittnad utmaning är digitala leveranskedjor. Enligt Tillväxtverket saknar många SMF:er kunskap om eller rutiner för att ställa säkerhetskrav på sina leverantörer. De pekar istället uppåt i leveranskedjan eller utgår från att deras leverantörer erbjuder säkra tjänster och produkter. Tredjepartsrisker underskattas, eller skattas inte alls.[168] Många små och medelstora företag är samtidigt ofta del av längre och ibland samhällskritiska leveranskedjor. Hotaktörer kan utnyttja mindre företag för att nå större eller samhällskritiska slutkunder i så kallade supply chain-angrepp, en typ av angrepp som ökat enligt Enisa.[169] Små och medelstora företag behöver alltså både ha kompetens och medvetenhet kring hur leveranskedjor kan påverka deras egen verksamhet och hur de, i egenskap av del i leveranskedjor, kan påverka andra.

Stöd och vägledning till svenska små och medelstora företag

Det finns många vägledningar, verktyg och stöd till svenska företag vad gäller digitalisering och säkerhet i stort och specifikt cybersäkerhet. Tillväxtverkets kartläggning från 2021 visar på en mängd olika stöd men lyfter också att få av dem har små och medelstora företag som utpekad målgrupp eller utgår från deras behovsbild.[170] Några av de stöd som finns är:

[166] https://www.mcf.se/sv/publikationer/verktyg-for-okad-motstandskraft-och-starkt-civilt-forsvar--arsrapport-it-incidentrapportering-2024/
[167] https://www.mcf.se/sv/publikationer/andringar-som-bade-hotar-och-skyddar-20-rekommendationer-for-sakrare-andringar-i-vara-informationssystem/
[168] https://tillvaxtverket.se/download/18.6855bfcf184896002ffc18/1668765886578/S%C3%A4ker%20digitalisering%20i%20sm%C3%A5%20och%20medelstora%20f%C3%B6retag.pdf
[169] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[170] https://tillvaxtverket.se/download/18.6855bfcf184896002ffc18/1668765886578/S%C3%A4ker%20digitalisering%20i%20sm%C3%A5%20och%20medelstora%20f%C3%B6retag.pdf

- Myndigheten för civilt försvars Cybersäkerhetskollen som mäter nivån på organisationers systematiska cybersäkerhetsarbete, samt ger stöd för förbättringsarbete.
- Myndigheten för civilt försvars metodstöd för systematiskt informationsarbete i organisationer.
- Myndigheten för civilt försvars tjänst Cybersäkerhetsrådgivningen, en kostnadsfri rådgivning inom systematiskt cybersäkerhetsarbete som är öppen för alla verksamheter.
- NCSC:s rapporter med analyser och rekommendationer, bland andra ”Cybersäkerhet i Sverige 2024” och ”Utpressningsangrepp, temafördjupning”
- Enisas guide ”Cybersecurity guide for SMEs”.
- SSF Stöldskyddsföreningens tjänst Säkerhetskollen.
- Enisas verktyg SecureSME
- Tillväxtverkets rapport ”Säker digitalisering i små och medelstora företag” som både innehåller kartläggning och rekommendationer.
- Cybernoden, den svenska kompetensgemenskapen för cybersäkerhet som drivs av RISE på uppdrag av NCC-SE, där alla organisationer som är intresserade av cybersäkerhet kan bli medlemmar och utbyta erfarenheter.

Kunskapen om, hur och i vilken utsträckning stöden används samt leder till förändrade beteenden är begränsad med få offentliga siffror. Cybernoden visar ett stigande antal medlemmar, vilket indikerar ett ökat intresse för cybersäkerhetsfrågor men djupare uppföljning saknas. 2024 genomförde NCC-SE en nationell utlysning för svenska SMF:er som ville bidra till att stärka Sveriges kapacitet och infrastruktur inom cybersäkerhet och beredskap. De 36 finansierade projekten handlade bland annat om arbete med reglering, utbildningsinsatser, cybersäkerhetskartläggning och hantering av risker. Utvärderingen visar att 57 procent av företagen förbättrat sin regelefterlevnad, 67 procent ökat sin förmåga att arbeta strukturerat med cybersäkerhet och 76 procent upplevt stärkt kundförtroende, men effekterna på långsiktiga beteendeförändringar är ännu oklara.[171]

Utöver det stöd som myndigheter tillhandahåller finns det även företag och högskolor som erbjuder utbildningar i cybersäkerhet till specifikt små och medelstora företag. Det genomförs även initiativ och projekt regionalt för att stärka cyberhygienen och -resiliensen hos SMF:er, bland annat håller science parks med flera workshops, samverkansforum och kurser.

Näringslivet ger även sitt stöd via handelskammare och intresseorganisationer som adresserar cybersäkerhet i artiklar, rapporter och vägledningar. De lyfter både

[171] https://www.ncc-se.se/siteassets/ansokningsprocessen/rapporteffektkartlaggningfstp2024.pdf

cyberhoten som svenska företag står inför och cybersäkerhet som en strategisk åtgärd för att stärka Sveriges konkurrenskraft. Det finns även branschföreningar som till exempel SOFF och SME-D som driver frågorna för säkerhets- och försvarsföretag, men även andra branschspecifika organisationer har forum för cybersäkerhet, till exempel Energiföretagen.

Regleringar som påverkar svenska små och medelstora företag

Nya regleringar på cybersäkerhetsområdet kommer att påverka många svenska små och medelstora företag. De nya kraven gör att cybersäkerhet blir en viktigare regelefterlevnadsfråga både gällande teknik och styrning.

Cybersäkerhetslagen är det hittills mest genomgripande ramverket för cybersäkerhet i Sverige. Det berör främst organisationer med samhällsviktig verksamhet men även leverantörer till dessa. SMF:er kommer att kunna omfattas indirekt då samhällsviktiga verksamheter kan ställa krav i enlighet med lagen på sina leverantörer för att säkerställa säkerheten i sina digitala leveranskedjor.

Utöver detta kan CER-direktivet, Cyberresiliensförordningen (CRA) och EU-förordningen för digital operativ motståndskraft (DORA) komma att påverka svenska SMF:er genom ökade krav på cybersäkerhet, riskhantering och rapportering, framförallt för de som levererar till samhällsviktiga verksamheter eller finanssektorn. Lagstiftning som AI-förordningen kommer också att ha inverkan genom att i sin tur ställa högre krav på transparens, datasäkerhet och ansvarsfull hantering av AI.

Utredningen om CRA[172], SOU 2025:115, bedömer att många SMF:er kommer att omfattas av den nya regleringen och att behovet av stöd till SMF:er är stort. Stödet behöver både vara stödjande resurser och kunskapshöjande insatser för att näringsliv och innovation inte ska hämmas.[173]

Analys av nuläget

Samhällets digitala transformation innebär stora möjligheter för svenska små och medelstora företag. Smidigare kommunikationsprocesser, underlättade flöden samt enklare kontakt med kunder och myndigheter bidrar till tillväxt och ökad internationalisering. Samtidigt är utmaningarna stora, inte minst vad gäller säkerhetsaspekterna. Det är positivt att många initiativ tas för att skapa vägledande material i allmänhet, och med SMF:er som målgrupp i synnerhet. Men materialet är utspritt, sällan målgruppsanpassat, upplevs svårt att hitta och begränsad

[172] EU:s cyberresiliensförordning
[173] https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2025/12/sou-2025115/

uppföljning på användning och effekt genomförs. De tydligaste utvecklingsområdena är:

1. Många små och medelstora företag har begränsade resurser vad gäller kompetens, tid och finansiering vilket gör det svårt att hitta, förstå och omsätta tillgängliga vägledningar och verktyg för cybersäkerhet. Orsaksbilden är bred och inbegriper bland annat låg insikt om behov av specialistkompetens, behov av att fokusera på kortsiktig affärsnytta framför regelefterlevnad samt utmaningar kopplade till att sätta sig in i ny teknik och säkerhetsfrågor när ens expertis ligger i andra sektorer. Konsekvensen blir att befintligt stöd inte nyttjas fullt ut och därmed inte skapar den företags- eller samhällsnytta som det finns potential för.
2. Det finns idag inte en aktör med tydligt uppdrag att framställa, samordna och målgruppsanpassa stöd till SMF:er när det kommer till systematiskt cybersäkerhetsarbete, utöver ett förslag i SOU 2025:115[174] om att ansvarig myndighet för NCC-SE[175] och PTS[176] ska ge ett samlat stöd till SMF när det gäller frågor som berör infrastruktur och livscykelhantering av produkter i enlighet med CRA. En orsak till detta är att ingen aktör fått i officiellt uppdrag att ta sig an frågan om ett samlat för cybersäkerhet i stort. Samtidigt har de organisationer som erbjuder vägledningar och verktyg begränsade uppdrag, resurser och/eller förståelse för företagens sinsemellan varierande behov. Detta leder till ett stort men spretigt stödutbud som är svårnavigerat för SMF:er samt försvårar avgörandet av vilka råd som är mest relevanta, hur initiativ hänger ihop eller varför motstridiga rekommendationer ibland ges. Konsekvenserna blir att företagen får svårt att hitta, använda och prioritera bland stöden vilket försvagar effekten av insatserna.
3. Bristen på cybersäkerhetskompetens både i företagsledningar och bland tekniska experter, något som både Enisa och NCSC lyft. Orsakerna handlar bland annat om ett snabbt ökande behov som inte taktats med antalet utbildade yrkespersoner. Det begränsade antalet specialister i Sverige gör det svårt för SMF:er att rekrytera kunnig personal, både till verksamhet och ledningar, samtidigt som ledningens engagemang ofta är avgörande för prioriteringen av cybersäkerhet. Konsekvensen blir att SMF:er har begränsad förmåga att säkerställa cybersäkerhet i sina tjänster och produkter vilket på sikt påverkar både cyberhygien, -resiliens och förtroende.
4. Små och medelstora företag är både leverantörer i komplexa leveranskedjor och köper tjänster och produkter med komplexa leveranskedjor. Kunskapen om och förmågan till att förstå de

[174] Statliga utredningen om CRA (EU:s cyberresiliensförordning)
[175] Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet.
[176] Post- och telestyrelsen

säkerhetsproblem som finns kopplade till leveranskedjor är begränsad, något som hänger ihop med SMF:ers utmaningar gällande brist på resurser och kompetens att omhänderta cybersäkerhetsperspektiv generellt. Utmaningen hänger också ihop med osäkerhet kring om och i så fall hur teknikföretag som levererar till SMF:er tar ansvar för att deras tjänster är säkra. Vissa tjänster och produkter är också så omfattande att det kan vara svårt för SMF:er att ställa krav på dem eller ha finansiella möjligheter att köpa säkra tjänster. Detta leder till SMF:er kan bli utsatta för sårbarheter och cyberhot genom de produkter och tjänster de köper och säljer, vilket kan leda till produktionsbortfall, störningar i samhällsviktiga tjänster och ekonomiska konsekvenser.

5. Små och medelstora företag behöver förhålla sig till många regelverk. Utöver cybersäkerhet kan det handla om arbetsmiljö, jämställdhet och hållbarhet. Orsakerna är att SMF:er omfattas av många regelverk för att säkerställa deras ansvarstagande med mera. Detta utgör ett problem genom att företagen måste ta till sig en stor mängd information eller nyttja verktyg och vägledningar från ett flertal myndigheter inom många olika ämnesområden, vilket leder till en risk för cybersäkerheten då den eventuellt bortprioriteras.
6. Det saknas ett skalbart ramverk för SMF:er som bygger på standardiserade säkerhetsåtgärder, en riskbaserad metod och detaljerad dokumentation för att skapa en systematisk och repeterbar säkerhetsprocess. Orsaken är att inget nationellt uppdrag getts eller initiativ tagits på området. Detta gör det svårare för företagen att driva ett cybersäkerhetsarbete utifrån deras förutsättningar.

Målbild 2029

2029 fortsätter samhällets digitala transformation att skapa möjligheter för svenska små och medelstora företag genom smidigare kommunikationsprocesser, underlättade flöden samt enklare kontakt med kunder och myndigheter vilket fortsätter bidra till tillväxt och ökad internationalisering. Detta sker genom att svenska SMF:er fortsätter omhänderta de möjligheter som digitalisering erbjuder på ett ansvarsfullt sätt, något som sker smidigare genom den kunskapsökning, ökade tillgång till stödmaterial och målgruppsanpassade processer som fortsatt utvecklas, bland annat utifrån insatserna som beskrivs nedan.

2029 erbjuds små och medelstora företag kvalitetssäkrat och målgruppsanpassat stödmaterial via svenska myndigheter. Detta övergripande stöd möter generella behov och utmaningar för att SMF:er ska hålla god cyberhygien och uppnå ökad cyberresiliens. NCSC har ansvar för att utveckla, förvalta och tillhandahålla stödet i nära samarbete de myndigheter som ansvarar för verksamt.se, det vill säga Tillväxtverket, Skatteverket och Bolagsverket. Stödet är en vidareutveckling av det

material som idag publiceras under rubriken Skydda företaget hos verksamt.se[177]. Den tydliga ansvarsfördelningen mellan myndigheterna har underlättat samverkan med intresse- och företagsorganisationer. Stödmaterialet som NCSC erbjuder fungerar som grund för andra initiativ där idéburna, kommersiella och i vissa fall offentliga aktörer kan nyttja grundstödet för att vidareutveckla och mer precist målgruppsanpassa, kompletterande stödmaterial eller -insatser. Genom tydliga referenser till NCSC kan användare av det vidareutvecklade stödet tillse att innehållet är aktuellt och relevant. Ett ytterligare relaterat stöd är NCSC:s och Upphandlingsmyndighetens stöd för cybersäker upphandling. För att underlätta för små och medelstora företag att förstå och agera på den nya regleringen som CRA gör gällande erbjuds också specifikt stöd inom dessa frågor. Till 2029 bistår NCSC med stödet, stödet har publicerats och används.

Till 2029 har EU:s arbete med förenkling av regler för stärkt konkurrens fortsatt.[178] Detta har bidragit till att minska den generella regelbördan för SMF:er. Samtidigt har den nationella digitala portalen för bland annat inrapportering av incidenter lanserats och utvecklats, något som underlättat för SMF:er att specifikt följa den reglering som berör cybersäkerhet oavsett om det gäller Cybersäkerhetslagen eller CRA. Portalen är utvecklad för att förenkla för SMF:er i enlighet med SOU 2025:115[179] problembeskrivning och föreslagna åtgärder.

2029 fortsätter nationella cybersäkerhetssatsningar underlätta för små och medelstora företag. Genom NCC-SE har SMF:er möjlighet att ansöka om medel för stärkt cybersäkerhetskapacitet och innovationsinsatser inom området. Den svenska kompetensgemenskapen Cybernoden, som drivs av RISE och inriktas av NCSC i sin roll som NCC-SE, har ett fortsatt tydligt uppdrag att samla svenska SMF:er med kompetens eller behov kring cybersäkerhet. Genom Cybernodens erbjudanden får SMF:er tillgång till kunskapshöjande insatser som relevanta webbinarier och temagrupper. Cybernoden initierar också samverkan mellan aktörerna för att se över möjligheter till gemensamma tekniska säkerhetslösningar.

Det vidareutvecklade stödet och den generella medvetandehöjningen kring cybersäkerhet som nämns i policyn om ökad medvetenhet har haft positiv inverkan på svenska SMF:er till 2029. Samtidigt har möjligheterna till utbildning ökat, vilket nämns i samma policy. En central aktör är Cybercampus som erbjuder introduktions-, fortsättnings- och avancerade kurser till företag och organisationer. Cybercampus stöd kompletteras också genom andra utbildningsinsatser och av andra utbildningsleverantörer. Tillgången till utbildning och kunskapshöjningen ger SMF:er ökad tillgång till kompetens, antingen inom sin egen organisation, via rekrytering eller inköp, exempelvis genom konsultinsatser. Genom Cybernoden och andra samverkansarenor uppmuntras så väl små och medelstora som stora

[177] https://verksamt.se/skydda-foretaget
[178] https://commission.europa.eu/law/law-making-process/better-regulation_sv
[179] Statliga utredningen om CRA (EU:s cyberresiliensförordning)

teknikföretag att ta ansvar för att erbjuda säkra tjänster vilket indirekt stärker SMF:ers cybersäkerhet genom säkrare it-tjänster.

Till 2028 har NCSC utrett om ett skalbart ramverk för SMF:er med syfte att stötta framdriften i deras cybersäkerhetsarbete utifrån deras förutsättningar kan skapa nytta och underlätta för svenska SMF:er. Ramverket ska bygga på standardiserade säkerhetsåtgärder, en riskbaserad metod och detaljerad dokumentation för att skapa en systematisk och repeterbar säkerhetsprocess. NCSC har tagit del av erfarenheter från andra europiska initiativ, exempelvis från Tyska Federala kontoret för informationssäkerhet (BSI). Om NCSC finner att ramverket är värdeskapande för målgruppen är utvecklingen av det påbörjad 2029.

Genom dessa insatser är det 2029 enkelt att hitta aktuellt, korrekt och relevant stödmaterial för svenska små och medelstora företag, både på generell nivå och till viss del i mer specifika frågor eller för specifika behov. Det är lätt för SMF:erna att avgöra om stödet är aktuellt genom kontinuerlig förvaltning hos NCSC, något som även de aktörer som vill vidareutveckla mer specifikt stöd kan luta sig mot. Floran av olika stöd är bred, från NCSC:s guider eller liknande, till temagrupper för diskussioner och webbinarier genom Cybernoden och riktade insatser genom aktörer som SSF Stöldskyddsföreningen. Det är samtidigt enkelt att hitta passande utbildningar, bland annat genom Cybercampus, och söka medel för stärkt cybersäkerhetskapacitet genom NCC-SE.

Åtgärder för att uppnå målbilden

1. Till 2029 har utmaningen med resursbrist hos SMF:er samt avsaknaden av ett samlat, målgruppsanpassat och tydligt stödmaterial eller stödinsatser till små och medelstora företag mötts genom att regeringen gett i uppdrag åt NCSC att utveckla och förvalta relevant stöd för svenska SMF:er. Uppdraget sker i nära samarbete med myndigheterna som ansvarar för verksamt.se, det vill säga Tillväxtverket, Bolagsverket och Skatteverket samt PRV för att säkra kompetens inom frågor som rör patent och immaterialrätt. För att nå cybersäkerhetsstrategins målbild om ökad cyberresiliens hos SMF:er samt tillgängligt stöd 2030 påbörjas arbetet senast 2027 med första lansering samma år. Stödet utvecklas och uppdateras agilt. NCSC får även i uppdrag att i sin roll som NCC-SE förse små och medelstora företag med stöd kopplat till CRA. För att säkerställa att företagen har goda förutsättningar att uppnå skyldigheterna när de planeras börja gälla fullt ut i december 2027 påbörjas arbetet 2026 och intensifieras 2027. Upphandlingsmyndigheten får i uppdrag att erbjuda stöd gällande cybersäkerhet inom offentlig upphandling med NCSC som samverkanspart som bistår med kompetens och kvalitetssäkring. Detta stöd omhändertas av policyn om cybersäker upphandling. Att utveckla och förvalta stödmaterial mot en så diversifierad målgrupp är resurskrävande, särskilt när det sker inom ett dynamiskt fält med

snabb utveckling samt i samverkan mellan flera myndigheter. Därmed tillfaller resurser berörda myndigheter i samband med uppdragen.

2. 2029 har bristen på cybersäkerhetskompetens både i företagsledningar och bland tekniska experter mötts genom de medvetandehöjande och utbildningsinriktade insatser som policyn om utbildning, forskning och innovation[180] lyfter. Samtidigt bidrar det nationella stöd som NCSC tillsammans med myndigheterna bakom verksamt.se samt tagit fram till att höja kunskapsnivån hos små och medelstora företag. Stödet ska vara genomtänkt och tas fram utifrån SMF särskilda förutsättningar och testas utav målgruppen för att säkerställa kvalitet och träffsäkerhet. Stödet är med fördel utformat som uppföljningsbara tjänster snarare än framförallt nedladdningsbart material. NCSC ska bidra med sakkunskap utifrån cybersäkerhetsområdet medan myndigheterna bakom verksamt.se ska ge sin särskilda expertis för att säkerställa att stödet som tillhandahålls ger effekt utifrån samtliga perspektiv. Även redan utvecklat stöd och utbildningar som legat hos Myndigheten för civilt försvar fortsätter skapa värde genom att utvärderas och uppdateras, exempelvis ”Kurs för beslutsfattare i samhällsviktiga verksamheter: Ledningsperspektiv på informations- och cybersäkerhet” [181], detta genom att flyttas över till NCSC:s regi i samband med myndighetsövergången 1 juli 2026. Kursen ska utgöra en grund för att skapa en liknande för SMF:er. Utbildningarna bidrar till att öka SMF kunskap, men ger även SMF möjligheten att utvecklas tillsammans med andra som står inför samma utmaningar genom utbyte under utbildningen. Till 2029 fortsätter SMF ges möjlighet att utvecklas inom cybersäkerhet genom att Cybernodens insatser för målgruppen. För att fortsätta upprätthålla det utbud av utbildningar som redan existerar för SMF får Cybercampus i uppdrag att bevaka och stötta dessa utbildningar särskilt.

3. Till 2029 har utmaningen med de många regelverk som SMF:er behöver förhålla sig till möts dels genom EU:s fortsatta arbete med regelförenkling, dels genom att NCSC fått i uppdrag att vidareutveckla och förvalta den nationella portal för inrapportering med mera som Myndigheten för civilt försvar lanserar under början av 2026. Genom att arbeta utifrån användares behov, iterativt och agilt skapas en portal som kan omhänderta informationsbehov, rapportering med mera i enlighet med ny lagstiftning eller ny reglering på cybersäkerhetsområdet.

4. Till 2029 har utmaningen med risker kopplade till små och medelstora företag inom komplexa leveranskedjor och köpare av tjänster och produkter med komplexa leveranskedjor mötts genom de rekommendationer som policyn om

[180] Policy för att främja och utveckla cybersäkerhetsutbildning, cybersäkerhetskompetens, medvetandehöjande åtgärder och forsknings- och utvecklingsinitiativ, samt vägledning om god praxis och kontroll för cyberhygien som riktar sig till medborgare, intressenter och entiteter.
[181] https://www.mcf.se/sv/utbildning--ovning/utbildning/alla-kurser/kurs-for-beslutsfattare-ledningsperspektiv-pa-informations--och-cybersakerhet/

leveranskedjor[182] tar upp men även genom att Cybernoden från 2026 aktivt används som arena för kunskapsutbyte och efterforskningar till gemensamma tekniska säkerhetslösningar genom samtal och utforskandet av temagrupper[183] samt för att uppmuntra alla typer av teknikleverantörer att erbjuda säkra tjänster, något som ny reglering och lagstiftning på området också kommer att kräva.

5. Avsaknaden av ett skalbart ramverk för SMF:er möts genom att NCSC utreder målgrupperna behov och påbörjar utveckling av ramverket om utredningen visar att ramverket skapar nytta hos väsentlig målgrupperna.

Indikatorer

Referenser

[182] Policy för cybersäkerhet i leveranskedjan för IKT-produkter och IKT-tjänster som används av entiteter när de tillhandahåller sina tjänster.
[183] Temagrupperna är reglerade och kräver att fyra medlemmar vill starta en för att det ska kunna startas i Cybernodens regi.

Främja ett aktivt cyberskydd

Enligt NIS 2-direktivets artikel 7.2 j) Riktlinjer för att främja ett aktivt cyberskydd.

Definitioner och begrepp

Skäl 57 i NIS 2-direktivet ger följande beskrivning av aktivt cybersskydd:

> I stället för reaktiva insatser innebär ett aktivt cyberskydd förebyggande, upptäckt, övervakning, analys och begränsning av överträdelser av nätverkssäkerheten, i kombination med användning av kapacitet som satts in inom och utanför det angripna nätverket.
>
> Detta kan bl.a. innebära att medlemsstaterna erbjuder vissa entiteter kostnadsfria tjänster eller verktyg, t.ex. självbetjäningskontroller, upptäcktsverktyg och borttagningstjänster. Förmågan att snabbt och automatiskt utbyta och förstå information om och analyser av hot, varningar om cyberverksamhet samt motåtgärder är avgörande för att med förenade ansträngningar lyckas förebygga, upptäcka, hantera och blockera attacker mot nätverks- och informationssystem. Ett aktivt cyberskydd bygger på en defensiv strategi som utesluter offensiva åtgärder.

Den svenska definitionen av aktivt cyberskydd:

> Aktivt cyberskydd är tekniska eller organisatoriska tjänster och verktyg som är kontinuerligt eller regelbundet tillgängliga och som, i realtid eller med en fastställd frekvens, övervakar, analyserar, informerar om och/eller ingriper i/vid cybersäkerhetsrelaterade risker, hot, sårbarheter, eller incidenter.

Andra centrala uttryck i policyn:

Leverantör av hanterade säkerhetstjänster (enligt definitionen i NIS 2-direktivet): en leverantör av hanterade säkerhetstjänster som utför eller tillhandahåller stöd för verksamhet som rör hantering av cybersäkerhetsrisker.

Utlokaliserad säkerhetstjänst: En tjänst som tillhandahålls av en leverantör av utlokaliserade driftstjänster och som innebär hantering av eller utgör stöd för hantering av cybersäkerhetsrisker.

I cybersäkerhetslagen (2025:1506) har uttrycket ”utlokaliserad säkerhetstjänst” ersatt NIS 2:s uttryck ”leverantör av hanterade säkerhetstjänster”.

Introduktion

Konceptet aktivt cyberskydd införs rättsligt för första gången i EU-direktivet 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2-direktivet). Direktivet specificerar att ”som en del av nationella cybersäkerhetsstrategier ska medlemsstater tillämpa policyer för ett aktivt

cybersskydd som en vidare defensiv strategi". Ett aktivt cyberskydd bygger på en defensiv strategi som utesluter offensiva åtgärder.

I Sverige innefattar ett aktivt cyberskydd en rad olika tjänster, i första hand automatiserade, som kan upptäcka, varna, filtrera, blockera och analysera händelser i nätverk och informationssystem. Den svenska definitionen av ett aktivt cyberskydd utgår från skäl 57 i NIS 2-direktivet.

Aktivt cyberskydd innefattar även nödvändiga organisatoriska förutsättningar såsom den kompetens som krävs för att använda tjänsterna och verktygen och för att omhänderta innehållet i dem. Det aktiva cyberskyddet syftar till att förbättra samhällets förmåga att förhindra och stå emot både antagonistiska och icke-antagonistiska respektive tekniska och icke-tekniska hot.

Den här policyn syftar till att definiera vad som är ett aktivt cyberskydd samt föreslår åtgärder 2026–2029 för att skapa förutsättningar för ett ändamålsenligt aktivt cybersskydd som motsvarar svenska samhällets behov och det aktuella och stundande cyberhotlandskapet. Policyn syftar även till att skapa förutsättningar för ändamålsenlig styrning, utveckling och samverkan efter behov. Avslutningsvis syftar policyn till att bidra till att svenska organisationer känner till samt nyttjar dessa tjänster efter behov, i syfte att bli mer motståndskraftiga mot cyberhot och it-incidenter.

Avgränsning

Ett aktivt cyberskydd utgör inte tjänster eller verktyg som enbart tillhandahålls vid enstaka tillfällen eller som nyttjas för underrättelse- eller brottsförebyggande arbete.

Andra policys inom ramen för den nationella cybersäkerhetsstrategin skapar förutsättningar för ett aktivt cyberskydd, och i policyn för aktivt cyberskydd lyfts aspekter som skapar förutsättningar och nytta för andra policyområden.

Nulägesbild

Aktivt cyberskydd är ett nytt begrepp och koncept som lanseras i NIS 2-direktivet. Det innebär att det inte finns en etablerad definition av vilka tjänster som begreppet aktivt cyberskydd inkluderar. Det saknas i dagsläget en heltäckande kännedom om den svenska marknaden av aktörer som erbjuder tjänster inom ramen för ett aktivt cyberskydd enligt definitionen i denna policy. Det innebär även att enskilda organisationer, särskilt små organisationer, kan sakna såväl kännedom som kompetens gällande de tjänster som erbjuds, liksom vilken nytta de tillför. Det saknas även kompetens om hur relevant kravställning görs för att

anskaffa dessa tjänster, använda tjänsterna samt hur resultaten av tjänsterna ska analyseras och omhändertas[184].

Viss kartläggning av tjänster som marknaden erbjuder har FOI publicerat i november 2025. Denna studie fokuserar dock i huvudsak på tjänster som skulle kunna vara aktuella i Försvarsmaktens verksamhet och exkluderar molntjänster och hanterade tjänster. Den redogör vidare för problematiken med att det saknas en entydig definition av begreppet *aktivt skydd*. Däremot argumenterar rapporten för att begreppet aktivt innebär att produkterna har en hög grad av automatisering.[185]

FOI har även undersökt förutsättningar för att använda de identifierade teknikerna. Där lyfts bland annat att arbetet med att införa och tillämpa (integrera) teknikerna kan vara omfattande. Det kan också vara svårt att bedöma svårigheten i att sköta driften av dessa programvaror.[1]

Enligt NIS 2-direktivet ska den nationella CSIRT-enheten utföra vissa uppgifter[186]. Det handlar om att övervaka och analysera cyberhot, sårbarheter och incidenter, samt tillhandahålla stöd till verksamhetsutövare avseende realtidsövervakning av nätverks- och informationssystem. Den nationella CSIRT-enheten ska även tillhandahålla varningar, larm och information till verksamhetsutövare och andra relevanta intressenter, om möjligt i realtid. Flera av de tjänster och verktyg som den nationella CSIRT-enheten har utvecklat för att fullgöra uppgifterna i direktivet bedöms även ingå i ett aktivt cybersskydd[187]. Utöver den nationella CSIRT-enhetens tjänster finns ytterligare ett antal tjänster från staten[188]. Vissa av dessa är kostnadsfria och andra erbjuds mot ersättning.

Utöver det statliga tjänsteerbjudandet finns det flera kommersiella aktörer på den svenska marknaden som erbjuder tjänster inom aktivt cybersskydd. Därtill finns ytterligare aktörer såsom stiftelser, intresseorganisationer, branschsamarbeten och ideella initiativ som erbjuder tjänster som bedöms ingå i aktivt cyberskydd.

Idag saknas en formaliserad samverkan kring aktivt cyberskydd, även om det förekommer samverkan som tangerar definitionen av aktivt cyberskydd. Exempelvis anordnar både NCSC och Myndigheten för civilt försvar ett antal samverkansforum för informationsdelning inom cybersäkerhet där erfarenheter och information på temat utbyts.[189] Dock görs detta utanför ramen för aktivt

[184] Resultatredovisning Cybersäkerhetskollen 2025.
[185] https://www.foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI-R--5797--SE
[186] Art. 11.3 NIS 2-direktivet.
[187] Se tjänster som erbjuds av Myndigheten för civilt försvar på sida 120.
[188] Se tjänster som erbjuds av Myndigheten för civilt försvar och Försvarets radioanstalt på sida 120.
[189] Några faciliteras av NCSC, några faciliteras av MCF och sedan finns det forum som faciliteras av andra där representanter från MCF eller NCSC deltar.

cyberskydd eftersom begreppet är nyetablerat. Samverkan inom dessa forum behandlar också ämnen som ligger utanför ramen för aktivt cyberskydd.

Det innebär att det saknas en tydlig, formaliserad och heltäckande nationell samverkan mellan stat, akademi och näringsliv om behovet av tjänsteutveckling och tjänstetillämpningar från cyberssäkerhetsforskning avseende aktivt cyberskydd som kan nyttjas i praktiken.

Statliga tjänsteerbjudanden inom aktivt cyberskydd idag

I dagsläget erbjuds följande tjänster av Myndigheten för civilt försvar:

- **ANTS-SE** (Automatiska Notifieringar av Tekniska Sårbarheter) erbjuder en informationsdelningstjänst som varnar anslutna organisationer då information upptäcks om tekniska företeelser som kan behöva åtgärdas, exempelvis om enheter anslutit till övertagna botnät, om servrar har sårbara mjukvaror eller om tjänster har sårbara konfigurationer. ANTS-SE är kostnadsfritt och tillgängligt för alla svenska organisationer som vill ha hjälp med övervakning av sina angreppsytor på internet. ANTS-SE lanserades i maj 2023.[190]
- **MISP-SE** är en nationell hotdelningsplattform där svenska verksamhetsutövare kan dela med sig av och nyttja andras hotinformation. Delningen sker via verktyget MISP (Malware Information Sharing Platform) som används för att samla in, lagra, analysera och dela information om cyberhot och incidenter. Den möjliggör strukturerad och standardiserad delning av hotindikatorer (IOC), såsom IP-adresser, domäner och skadlig kod. MISP stödjer både manuell och automatiserad hantering av information, vilket gör det lättare att snabbt reagera på nya hot. CERT-SE förvaltar MISP-SE som lanserades under 2026.
- **Myndigheten för civilt försvars lägesbedömning cyber** är myndighetens lägesuppfattning inom cybersäkerhetsområdet, vilken genomförs via videomöte och utskick två gånger i månaden med cirka 500 aktörer inom både privat och offentlig sektor. Myndigheten för civilt försvars lägesbedömning cyber har erbjudits sedan 2023.
- **Cybersäkerhetskollen** är samlingsnamnet för Myndigheten för civilt försvars cybersäkerhetsmätningar inom informationssäkerhet, it-säkerhet, ot-säkerhet och säkerhet för digitala leveranskedjor. Cybersäkerhetskollen mäter nivån på verksamhetens systematiska cybersäkerhetsarbete, samt ger stöd för förbättringsarbete. Cybersäkerhetskollen genomförs med två års intervall och har erbjudits sedan 2021.[191]

[190] https://cert.se/rad-och-stod/ants/
[191] https://www.msb.se/cybers%C3%A4kerhetskollen

Försvarets radioanstalt tillhandahåller följande tjänst inom aktivt cyberskydd:

- **TDV** är ett tekniskt detekterings- och varningssystem till de mest skyddsvärda verksamheterna bland statliga myndigheter och enskilda verksamhetsutövare. Detta system erbjuds till verksamheter som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Det innebär att det endast är en begränsad mängd verksamheter som kan ta del av detta erbjudande för att stärka sitt aktiva cyberskydd.

Privata tjänsteerbjudanden inom aktivt cyberskydd

Privata aktörer erbjuder bland annat tjänster för upptäckt, varning, analys och informationsdelning av hot, intrång, överbelastning, liksom filtreringstjänster, t.ex:

- Security Operations Centers (SOC)
- Managed Detection and Response (MDR)
- Security Information och Event Management-verktyg (SIEM-verktyg)
- Threat Intelligence Platform (TIP)
- Intrångsdetekteringsverktyg (IDS/IPS)
- Skydd mot överbelastningsangrepp (DDOS-skydd)
- Verktyg för data loss prevention (DLP)

Internationell utblick

Det finns ett flertal internationella initiativ som kan ses som tjänster inom aktivt cyberskydd utifrån policyns definition. Enisa har kartlagt utbud och efterfrågan av hanterade säkerhetstjänster inom EU.[192] Kartläggningen visar att användningen av hanterade säkerhetstjänster är låg. Bland de huvudsakliga skälen till detta anges kostnader, brist på intern kompetens, samt svårigheter att skräddarsy och integrera lösningarna.

I Belgien har det belgiska cybersäkerhetscentret (CCB) definierat vad de anser utgör aktivt cyberskydd i en nationell policy.[193] Utöver de tjänster som redan täcks av det svenska, statliga tjänsteerbjudandet tillhandahåller de även ett DNS-skydd som hindrar en internetanvändare från att besöka skadliga webbplatser. NCSC-UK[194] erbjuder en rad olika tjänster och verktyg inom sitt program för aktivt cybersskydd, vilka är tillgängliga på NCSC-UK:s webbplats. Exempelvis erbjuds självbetjäningskontroller, DNS-skydd, e-postskydd och tjänster avseende tidiga varningar.

[192] https://www.enisa.europa.eu/publications/managed-security-services-market-analysis
[193] https://ccb.belgium.be/sites/default/files/2024-10/ACP_Policy_Document_EN.pdf
[194] https://www.ncsc.gov.uk/section/active-cyber-defence/services

Inom ramen för EU:s Cybersäkerhetsreserv upphandlar Enisa betrodda leverantörer av hanterade säkerhetstjänster. Dessa kan avropas av verksamhetsutövare i medlemsstaterna vid betydande incidenter.[195]

Regelbundet återkommande cyberövningar är också ett verktyg inom aktivt cyberskydd. I USA tillhandahåller CISA den återkommande övningen Cyber Storm[196] där organisationer inom både privat- och offentlig sektor övar på att utbyta och förstå information samt hantera cyberhot och incidenter under en simulerad storskalig cyberincident för att öka förmågan att förebygga, upptäcka och hantera liknande situationer i verkligheten. I EU genomförs övningen Cyber Europe[197] vartannat år i samma syfte.

Analys av nuläget

Det är positivt att staten erbjuder ett antal tjänster inom ramen för ett aktivt cyberskydd samt att ytterligare några tjänster planeras att erbjudas. Det är även positivt att näringslivet bidrar med tjänster inom aktivt cyberskydd som kompletterar det statliga tjänsteutbudet.

Det är vidare positivt att det finns internationella och europeiska aktörer som erbjuder tjänster för aktivt cyberskydd till svenska organisationer. Samtidigt finns en risk att såväl politiska förändringar som marknadsförändringar i omvärlden påverkar tillgången till dessa tjänster. Att många hanterade säkerhetstjänster kontrolleras av entiteter utanför EU kan vara en utmaning för den digitala suveräniteten.

Det är negativt att det inte finns en samlad bild över tjänsterna och tjänsteleverantörerna inom aktivt cyberskydd i näringslivet idag. Detta leder till att det är svårt att bedöma om dessa tjänster är tillräckliga sett till cyberhotlandskapet och samhällets behov samt huruvida de används i tillräcklig utsträckning för att ge önskvärd effekt. Orsaken till det är att ”aktivt cyberskydd” först nu har formaliserats som begrepp.

Det är negativt att det inte finns tillräcklig kunskap och kännedom om tjänsterna det vill säga vad tjänsterna är, vad de innebär och hur de kan stötta enskilda verksamheter i samhället, men även om kostnaderna för användning av dessa tjänster. Detta kan bero på att marknaden är under uppbyggnad och formaliseringen av begreppet. Det resulterar dock i att tjänsteutbudet inte fullt nyttjas eller utvecklas utifrån behovet. Verksamheter nyttjar tjänster och varumärken de känner igen på grund av att man inte vet vad som finns, vad tjänster är eller har kännedom om det egna behovet. Det är även negativt att

[195] https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cybersecurity-reserve
[196] https://www.cisa.gov/resources-tools/programs/cyber-storm
[197] https://www.enisa.europa.eu/topics/skills-and-competences-for-companies/cyber-europe

enskilda organisationer, särskilt små, saknar kunskap om hur de kan ställa relevanta krav och använda tjänsterna samt analysera och omhänderta resultatet av dem.

Det är negativt att det saknas tillräckligt underlag för att bedöma i vilken utsträckning, framförallt de kommersiella, tjänsterna används och vilken effekt de har. Detta innebär att det är svårt att bedöma vilka satsningar som bör genomföras inom området. För de etablerade, statliga tjänsterna förekommer en löpande uppföljning av användning och, där det så är möjligt, effekt.

Det är negativt att det saknas en formaliserad, strategisk samverkan mellan myndigheter, akademi och näringsliv samt en gemensam målbild för tjänsteutveckling inom aktivt cyberskydd. Orsaken till att det saknas är att området är nytt och inte etablerat än. Det får konsekvensen att tjänsteutvecklingen inom aktivt cyberskydd riskerar att utformas på ett ineffektivt, icke-målmedvetet eller samordnat sätt utan förankring i det aktuella cybersäkerhetslandskapet.

Det är negativt att organisationer inte avsätter tillräckliga resurser för det förebyggande cybersäkerhetsarbetet. Det innebär bland annat att de inte kan nyttja de tjänster som erbjuds fullt ut. Detta kan dels bero på att verksamheter väljer att kortsiktigt prioritera kärnverksamheten. Ytterligare en orsak kan vara att det under lång tid saknats reglering som kräver att verksamheter vidtar tillräckliga säkerhetsåtgärder. Det kan också bero på den rådande kompetensbristen inom hela cybersäkerhetsområdet - något som gör det svårt för organisationer att rekrytera personer med tillräcklig kompetens för att driva cybersäkerhetsarbetet till den mognadsnivå som krävs för att implementera den typen av tjänster. Det kompenseras delvis genom att flertalet av de statliga tjänster som erbjuds på basis av uppdrag och reglering till stor del är kostnadsfria. Användandet är emellertid ändå förknippat med vissa osynliga kostnader som följer av de organisatoriska förutsättningar och den kompetens som behövs för att använda tjänsterna.

Målbild 2029

År 2029 erbjuder staten flera tjänster inom ramen för aktivt cyberskydd. De statliga tjänsterna används i hög utsträckning och ger positiva effekter i organisationers operativa cybersäkerhetsarbete. Det är tydligt för svenska organisationer vilka tjänster inom aktivt cyberskydd som statliga aktörer erbjuder och vad de innebär.

År 2029 har CERT-SE utökat sitt tjänsteutbud med beaktande av mandaten i NIS 2 och genom omvärldsanalys över tjänsteutbudet hos andra nationella CSIRT-enheter. En av de nya tjänsterna som lanserats är DNS-SE, som genom ökad förmåga att upptäcka och blockera cyberhot i realtid utökar tjänsteutbudet inom aktivt cyberskydd. Utöver DNS-SE har även SOC-SE lanserats. SOC-SE är beställningsbara tjänster inom it-, ot- och nätverksövervakning som tillhandahålls

av privata aktörer på uppdrag av CERT-SE. SOC-SE syftar till att höja detektionsförmågan hos verksamhetsutövare. NCSC har ökat sin närvaro inom övningsområdet och erbjuder regelbundet återkommande cybersäkerhetsövningar som övar verksamheter både i det offentliga och näringslivet.

De tjänster och erbjudanden som finns 2029 svarar mot samhällets behov. Utveckling av nya tjänster sker proaktivt och drivs av ett tydligt definierat samhällsbehov, som inhämtas från näringsliv, stat och akademi, givet det aktuella cyberhotlandskapet. Det finns en samlad bild av hur användningen av tjänster inom aktivt cyberskydd ser ut. Effekterna av användningen följs upp löpande. Det finns också en tydlig bild av vilka tjänster inom aktivt cyberskydd som bidrar till ökad säkerhet hos enskilda organisationer.

Svenska organisationer nyttjar 2029 tjänster inom aktivt cyberskydd i syfte att stärka sin digitala motståndskraft och minska förekomsten och konsekvenserna av it-incidenter. Även mindre resursstarka organisationer inför och använder tjänster inom aktivt cyberskydd. De har den kompetens som krävs för att anskaffa, använda och analysera resultaten från tjänsterna.

2029 finns en formaliserad strategisk privat-offentlig samverkan för aktivt cybersskydd där stat, akademi och näringsliv identifierar behov och nyttjar innovation för att utveckla tjänsteutbudet för aktivt cyberskydd. Denna etablerade samverkan bidrar till att dela information om befintliga tjänster, utbyta erfarenheter och kartlägga behovsgap i syfte att skapa en tydlig struktur och inriktning kring den nationella tjänsteutvecklingen.

2029 har möjligheterna för att skapa stöd för upphandling av aktivt cyberskydd utretts. Utredningen har undersökt om vägledning och förenklade processer såsom statliga ramavtal för upphandling av aktivt cyberskydd kan stötta svenska organisationer att nyttja tjänster lättare.

2029 går det på ett enkelt sätt för näringslivet att ansöka om finansiering till vidareutveckling av tjänsteutbud inom ramen för aktivt cyberskydd. Finansieringen nyttjar både statliga och EU-medel.

2029 har en utredning som utreder behovet och möjligheten för certifiering av tjänster för aktivt cyberskydd genomförts. Utredningen ska ha sin grund i samhällets behov av kvalitetssäkra digitala produkter och tjänster samt hur det kan förenkla för tjänsteleverantörer att uppfylla krav.

Åtgärder för att uppnå målbilden

1. CERT-SE ska komplettera befintligt tjänsteutbud genom DNS-SE. Tjänsten ska användas av verksamheter för att filtrera bort skadligt innehåll genom att stoppa användares åtkomst till skadliga webbplatser och därigenom förebygga att it-incidenter äger rum. CERT-SE ska också, under 2026, komplettera sitt utbud med

tjänsten SOC-SE som är beställningsbara tjänster inom it-, ot- och nätverksövervakning som tillhandahålls av privata aktörer på uppdrag av CERT-SE. SOC-SE syftar till att höja detektionsförmågan hos verksamhetsutövare.

2. NCSC ska ta fram en regelbundet återkommande cybersäkerhetsövning som involverar verksamhetsutövare som träffas av Cybersäkerhetslagen (NIS 2). Övningen ska aktivera den nationella cyberkrishanteringsplanen för att även öva beroendena mot EU.

3. NCSC ska under 2026 komplettera Cybersäkerhetskollen med frågor som berör organisationernas användning av tjänster för aktivt cyberskydd från såväl statliga som privata aktörer. Frågorna ska undersöka vilka tjänster som finns, i vilken utsträckning de används samt vilka effekter de ger.

4. NCSC ska under 2026–2027 kartlägga marknaden av leverantörer och tjänster för aktivt cyberskydd för att undersöka utbudet. Kartläggningen ska även undersöka abonnemangserbjudande och kostnader för aktivt cyberskydd. En uppföljande kartläggning ska göras under 2029 för att se om utbudet ökat i enlighet med övriga insatser för att öka utbudet av leverantörer och tjänster.

5. Under 2026–2027 ska NCSC ska utreda möjligheten att ta fram stöd kring aktivt cyberskydd som en del av organisationers arbete med säkerhetsåtgärder för ett systematiskt cybersäkerhetsarbete. Stödet ska ge vägledning och kommunicera hur organisationer kan implementera och nyttja de statliga tjänster som erbjuds. Under kommande år, 2027–2029, kompletteras denna vägledning årligen baserat på resultaten av Cybersäkerhetskollen och omvärldsbevakning av tjänster från andra aktörer.

6. NCSC ska under 2026 arbeta med samverkan kring aktivt cyberskydd för att stärka koordineringen mellan stat, näringsliv och akademin för utvecklingen av tjänsteutbudet. En strategisk privat-offentlig samverkan ska inrättas och NCSC ska stötta Cybernoden[198] och Cybercampus[199] i främjandet av ett aktivt cyberskydd i Sverige. Cybernoden ska nyttjas som plattform för att lyfta det aktiva cyberskyddet möjliga stöd för svenska organisationer genom samtal och webbinarier på området, som en del av ledet för att stärka banden mellan stat, näringsliv och akademin. Cybercampus ska nyttjas för att stärka tjänsteutvecklingen av aktivt cyberskydd och säkerställa att det sker i linje med framtida risker och hot. Samverkan inom ramen för Cybercampus säkerställer att utvecklingen av erbjudna tjänster ska ske i linje med genomförd forskning och annan beprövad erfarenhet, då Cybercampus är ett samarbete mellan universitet, institut, myndigheter och

[198] Cybernoden är den nationella kompetensgemenskapen inom ramen för EU-projektet ECCC. Cybernoden är Sveriges nationella kompetensgemenskap inom cybersäkerhetsforskning och innovation och drivs av RISE på uppdrag av NCC-SE inom ramen för ECCC, och är finansierat av Vinnova.
[199] Cybercampus Sverige är ett nationellt initiativ som bedriver agil och banbrytande forskning, innovation och utbildning inom cybersäkerhet och cyberförsvar.

företag i hela Sverige. Cybercampus ska undersöka om aktivt cyberskydd kan undersökas närmare och vara ett tema för framtida samtal och kurser.

7. Fler insatser för att underlätta upphandling av aktivt cyberskydd genomförs. För att stötta upphandling och avrop av aktivt cyberskydd för statliga myndigheter ska ansvarig myndighet under 2027 undersöka möjligheterna för att genomföra en förstudie kring behov och förutsättningar för ett nytt ramavtalsområde om aktivt cybersskydd. För att förenkla marknaden för tjänsteleverantörer och köpare ska NCSC tillsammans med ansvarig myndighet till 2029 utreda möjligheterna att ta fram vägledning för upphandling för att stötta samhället i att upphandla aktivt cyberskydd.[200]

8. Staten ska underlätta finansieringen av näringslivets vidareutveckling av tjänsteutbud av aktivt cyberskydd genom NCC-SE:s utlysningar. NCC-SE ska därför i ett första led utreda behovet av finansiering av aktivt cyberskydd. Utredningen ska se om förenklade processer och ökade möjligheter till statlig finansiering och nyttjandet av EU-medel kan stötta marknaden i utvecklingen av nya tjänster.

9. NCSC ska tillsammans med ansvarig myndighet för genomförande av cybersäkerhetscertifieringar utreda behovet av och möjligheten till certifiering av tjänster som levereras inom ramen för aktivt cyberskydd. Utredningen ska se över köpares behov av kvalitetssäkring av tjänster och möjligheterna för en svensk certifieringsmodell.

Indikatorer

Referenser

[200] För förslag på cybersäkerhetsrelaterade krav vid upphandling se Policy för att inkludera och specificera cybersäkerhetsrelaterade krav för IKT-produkter och IKT-tjänster vid offentlig upphandling, inbegripet vad gäller cybersäkerhetscertifiering, kryptering och användning av cybersäkerhetsprodukter med öppen källkod.

Myndigheten
för civilt försvar