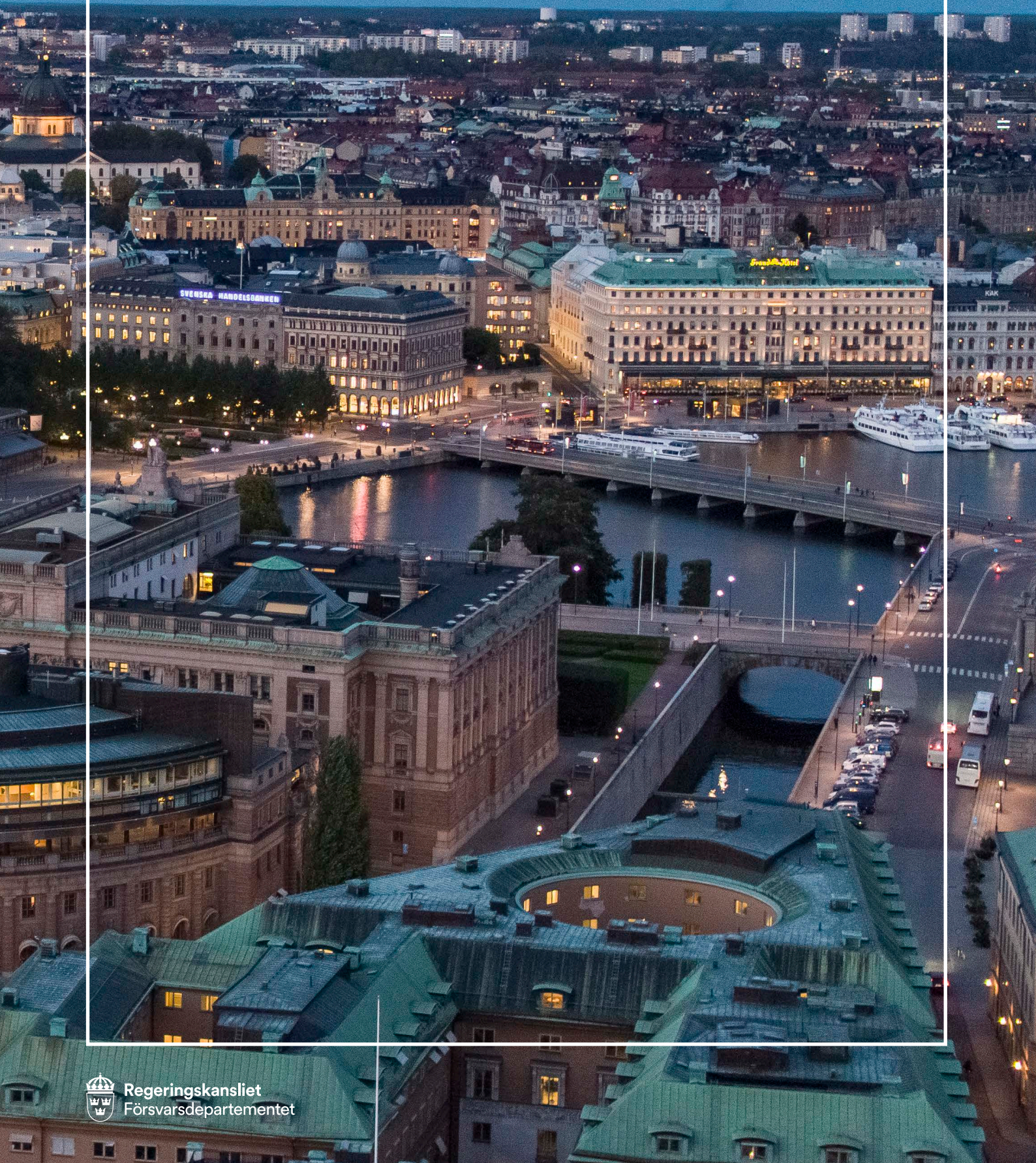
En ny era av cybersäkerhet

Nationell strategi för cybersäkerhet 2025-2029



Regeringskansliet
Försvarsdepartementet

Innehåll

Produktion: Alice Thoms och Niklas Forsström/Regeringskansliet 2025
Foto: Niklas Forsström/Regeringskansliet (omslag), Kristian Pohl AB/Regeringskansliet (sida 7)

Digitalt dörrlås.

Foto: Maskot/Folio/Image Bank Sweden

Förord

Carl-Oskar Bohlin
Minister för civilt försvar

Tiden för cyberpassivitet är förbi. Digital teknik berör numera närmast varje aspekt av det svenska samhället och ekonomin och den tekniska utvecklingen sker i fortsatt rekordfart. Det finns inga indikatorer på att det kommer förändras. Snarare står vi inför fortsatt acceleration. I takt med att det säkerhetspolitiska läget har försämrats och cyberhoten ökat, både sett till antal och komplexitet, ställs allt högre krav på Sveriges förmåga att säkra, skydda och stärka samhällets funktioner – även i cyberdomänen.

Sverige har länge dragit stor nytta av digitaliseringens möjligheter, men historiskt sett har cybersäkerhet ofta fått stå tillbaka för andra prioriteringar. Det är inte längre ett alternativ. Dagligen utsätts myndigheter, företag och enskilda individer för cyberangrepp i varierande omfattning, och mycket talar för att hotet kommer fortsätta öka. AI, maskininlärning och framtida kvantdatorer är fantastiska tekniker, men medför också ytterligare risker. Cybersäkerhet kan därför inte längre betraktas som enbart en teknisk fråga; i dag är det en grundpelare för vårt samhälles motståndskraft och en central del av det moderna civila försvar som nu byggs upp.

Den nya nationella cybersäkerhetsstrategin har utarbetats med viktiga bidrag från aktörer i både offentlig och privat sektor. Under arbetets gång har ett entydigt budskap blivit tydligt: det är brådskande att gå från ord till handling och höja Sveriges cybersäkerhetsförmåga. Den här strategin och den tillhörande handlingsplanen utgör därför en tydlig ambitionshöjning från regeringens sida och vilar på insikten att ett starkt samarbete, särskilt mellan offentliga och privata aktörer, är avgörande för att Sverige ska vara motståndskraftigt i en snabbt föränderlig, teknologidriven värld.

Denna strategi är en viktig pusselbit i det krafttag som regeringen nu genomför för ökad cybersäkerhet, men dokumentet är inte mycket värt utan konkret genomförande, faktisk förmågehöjning och uppföljning. Därför vill jag uppmana våra myndigheter, näringslivet och alla medborgare att inse att var och en – precis som för alla delar av totalförsvaret – också spelar en avgörande roll för Sveriges cybersäkerhet. Endast tillsammans kan vi säkerställa att Sverige står väl rustat för att möta både dagens och morgondagens utmaningar på cyberområdet.

Modern infrastruktur.

Foto: Felix Gerlach/Image Bank Sweden

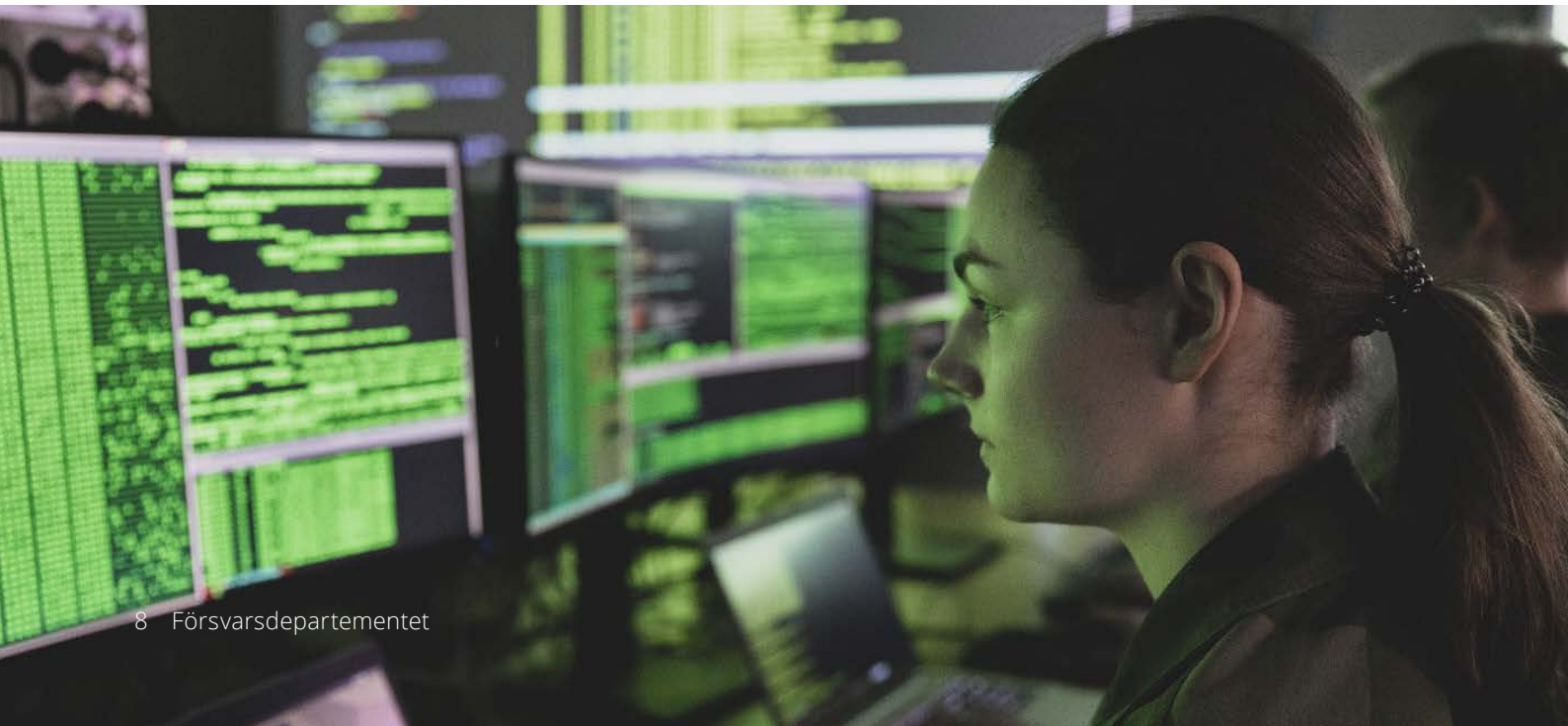
Vision

Regeringens vision är ett motståndskraftigt Sverige med en hög nivå av cybersäkerhet[1], där samhällsviktig verksamhet kan upprätthållas även vid cybersäkerhetsincidenter. För att uppnå denna vision krävs ett förstärkt cybersäkerhetsarbete och ett fördjupat och målinriktat samarbete mellan staten, näringslivet och akademin. Sverige ska dra full nytta av internationella samarbeten på cybersäkerhetsområdet inom EU, Nato och bilateralt med partnerländer för att aktivt stärka såväl vår nationella cybersäkerhet som den hos andra medlemsstater, allierade och partners.

Visionen understryker vikten av att få grundläggande och förstärkt cybersäkerhet på plats, samt vikten av fungerande samarbete mellan nyckelaktörer inom cybersäkerhetsområdet, såväl i fredstid som i krig. Ett välfungerande Nationellt cybersäkerhetscenter (NCSC) som bidrar till att samordna samhällets arbete med att stärka den nationella cybersäkerhetsförmågan behövs och kommer också sektorsansvariga myndigheter till gagn i deras arbete med att ta fram välanpassade krav. Detta är en grundförutsättning för hög cybersäkerhet och höjer den nationella förmågan att förebygga, förbereda sig för, förstå, bemöta och utvärdera cybersäkerhetsincidenter. Det bidrar också till en robust bas för det civila försvaret och till ett effektivt cyberförsvar samt bidrar till att stärka svenska företags position och konkurrenskraft.

Allt detta ska sammantaget leda till ett säkrare Sverige.

1 Cybersäkerhet: denna strategi använder likt NIS 2-direktivet termen ”cybersäkerhet” i stället för termen ”informations- och cybersäkerhet”.



Cybersoldat.

Foto: Joel Thungren/Försvarsmakten

Den nationella cybersäkerhetsstrategins utgångspunkter

Den nationella strategin för cybersäkerhet utgår från nationella behov och från NIS 2-direktivet och dess allriskperspektiv för att hantera en bredd av utmaningar såsom kompetensbrist, komplex reglering, sårbara leveranskedjor och bristande systematiskt cybersäkerhetsarbete. Mot bakgrund av det säkerhetspolitiska läget fokuserar strategin därtill i vissa delar särskilt på antagonistiska hot i hela hotskalan.[1] Strategin ersätter den tidigare strategin Nationell strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213).

Ansvarsprincipen gäller även på cyberområdet
Vid en cybersäkerhetsincident kan en krissituation uppstå som konsekvens och ansvarsprincipen därmed bli tillämplig inom den offentliga förvaltningen. Principen 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 särskilda fall, till exempel vid det som i NIS 2-direktivet benämns storskaliga cybersäkerhetsincidenter och kriser, ska dock en eller flera behöriga cyber-krishanteringsmyndigheter ansvara för nationell hantering. Detta gäller till exempel omfattande eller gränsöverskridande incidenter.

Ett systematiskt och riskbaserat cybersäkerhetsarbete hos samhällets alla organisationer utgör, tillsammans med säkerhetsskydd och cyberförsvar, Sveriges nationella motståndskraft på cybersäkerhetsområdet. Organisationer används i denna strategi som samlingsbegrepp och avser allt från statliga myndigheter och statligt ägda bolag till bland annat kommuner, regioner och privata och kommunala bolag. Med ett systematiskt cybersäkerhetsarbete åsyftas att skyddsåtgärder prioriteras systematiskt och utifrån en bedömning av vilka risker som är mest sannolika och har störst potentiell påverkan. Säkerhetsskydd avser skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter. Säkerhetsskydd inkluderar även de skyddsåtgärder som genomförs inom informations- och cybersäkerhetsområdet för att upprätthålla säkerhetsskyddet. Säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2021:955) gäller bland annat för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet. Cyberförsvar är en integrerad del av det militära försvaret och bidrar till Sveriges samlade förmåga att möta ett väpnat angrepp. Cyberoperationer är en lika självklar del av krigföringen i dag som mark-, sjö-, luft- och rymdoperationer. I fredstid kan Försvarsmaktens cyberförsvarsresurser användas för att stödja samhället under kriser eller andra allvarliga händelser.

1 I avsnitt 3 Cybersäkerhetslandskapet redogör regeringen för ett antal olika utmaningar, sårbarheter och hot som utgör strategins omvärldskontext.

Målgrupp

Den nationella strategin för cybersäkerhet och den tillhörande handlingsplanen ska vara av värde för hela samhället och alla typer av organisationer, såväl deras ledningar som de funktioner som arbetar med cybersäkerhet. Strategins primära målgrupp är dock myndigheterna med särskilt ansvar för verksamhet som bedrivs inom ramen för NCSC, och tillsynsmyndigheter inom den samlade cybersäkerhetsregleringen samt andra organisationer som ingår i beredskaps- och NIS 2-sektorerna.

Nationell politik för cybersäkerhet

Cybersäkerhet är ett område som sträcker sig över flera fält, politikområden och sektorer. Cybersäkerhetsfrågorna kräver således ett tvärsektoriellt arbete utifrån en rad olika kompetenser. Denna strategi kommer att utgöra regeringens långsiktiga inriktning för det systematiska arbetet med cybersäkerhet tillika regeringens politik för cybersäkerhet. Regeringens arbete med att stärka och bidra till Sveriges cybersäkerhet återspeglar sig även i bland annat propositionen Totalförsvaret 2025–2030 (prop. 2024/25:34). I propositionen konstateras det att informations- och cybersäkerhet är en viktig förutsättning för hela totalförsvaret inklusive det militära cyberförsvaret. Vidare betonas vikten av att Försvarsmakten i fred kan bidra till cybersäkerhetsarbetet. Utrikes- och säkerhetspolitiska aspekter av cyberfrågor behandlas primärt i regeringens strategi Sverige i en digital värld – en strategi för Sveriges utrikes- och säkerhetspolitik inom cyberfrågor och digitala frågor (UD2024/16802). Den strategin och den nationella strategin för cybersäkerhet är ömsesidigt förstärkande. De båda strategierna har flera beröringspunkter. Exempelvis utgör nationell förmåga inom lägesmedvetenhet, attribuering och svarsåtgärder en viktig del i utrikes- och säkerhetspolitiskt bemötande av cyberhotaktörer. Koordinering av utrikes- och säkerhetspolitiken med åtgärder på nationell nivå är en förutsättning för samlad hantering av så kallade offentliga utpekanden och bidrar till stärkt medvetenhet och motståndskraft.

Regeringens nationella säkerhetsstrategi (skr. 2023/24:163) sätter ramarna för arbetet med nationell säkerhet. Den beskriver de prioriteringar och principer som ligger till grund för Sveriges säkerhet och är utgångspunkten för de överväganden som görs i denna strategi. Den nationella säkerhetsstrategin anger att åtgärder för att samhällsviktiga och samhällskritiska verksamheter ska bli mer motståndskraftiga mot allvarliga störningar i fredstid är en prioriterad del av arbetet med att stärka det civila försvaret. Samtidigt betonar regeringen i den nationella säkerhetsstrategin att Sveriges nationella säkerhet är en angelägenhet för alla i vårt samhälle. En målbild är även att säkerhetshotet från auktoritära stater som Kina, Ryssland och Iran prioriteras och hanteras i samarbete med demokratiska länder. Av strategin framgår att regeringen avser att stärka förmågan att identifiera, hantera och bemöta hybridhot och angrepp, inklusive cyberangrepp.

Statsminister Ulf Kristersson i EU-parlamentet under Sveriges ordförandeskap.

Foto: Eric Vidal/EU

Regeringen inledde under 2023 ett arbete med att utveckla NCSC med målet att centret bland annat ska utgöra navet i det nationella cybersäkerhetsarbetet. Under 2023 tillsattes en så kallad bokstavsutredning med uppdrag att se över centrets verksamhet (Fö 2023:A). Utifrån den utredningen har regeringen beslutat att NCSC från och med den 1 november 2024 ska finnas inom Försvarets radioanstalt (FRA) samt att NCSC:s chef ska utses av regeringen. Utredningens övriga förslag bereds inom Regeringskansliet och berörs därför inte närmare i denna strategi.

I NIS 2-direktivet fastställs åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå i hela unionen. Regeringen tillsatte under 2023 en utredning för att bland annat föreslå de anpassningar av svensk rätt som bör göras till följd av direktivet och utredningen överlämnade i mars 2024 sitt delbetänkande (SOU 2024:18). Ansvarsförhållanden för de aktörer som omfattas av NIS 2-direktivet kommer att definieras i nationell reglering som införlivar direktivet i Sverige. I strategins bilaga 2 ges en nulägesbeskrivning av de centrala aktörer som har särskilda roller och ansvar att bedriva tillsyn, stötta och samordna arbetet med cybersäkerhet.[1]

Utöver denna cybersäkerhetsstrategi avser regeringen även att ta fram en strategi i enlighet med CER-direktivet[2]. Cybersäkerhetsområdet har dessutom naturliga kopplingar till frågor om digital omställning och digital infrastruktur, vilket kommer att beröras ytterligare i regeringens kommande digitaliseringsstrategi.

1 Bilagan utgår till del från den nationella reglering som införlivade NIS-direktivet och kommer att uppdateras när bland annat implementeringen av NIS 2-direktivet har fastställt ansvarsförhållandena inom svensk cybersäkerhet.

2 CER- och NIS 2-direktiven kompletterar varandra och ställer krav på samstämmighet. Exempelvis ska entiteter som identifierats som kritiska enligt CER-direktivet anses vara väsentliga enligt NIS 2-direktivet. Vidare ska nationella strategier antas som innehåller bland annat strategiska mål i syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå (NIS 2) respektive en hög grad av motståndskraft (CER).

Internationell kontext för nationell cybersäkerhet

Sveriges cybersäkerhet och reglering på området styrs delvis nationellt men också i ökande grad av den internationella kontexten. Sveriges cybersäkerhetspolitik påverkas av internationell reglering, styrande dokument, policyer och standarder. På lagstiftningsområdet styrs utvecklingen främst av EU-samarbetet. EU-kommissionen har tagit flera initiativ till reglering och normgivning inom cybersäkerhet och digitala frågor, inte minst NIS 2-direktivet. Vidare finns cyberresiliensförordningen och cybersäkerhetsakten, vilka båda är direkt tillämpliga i EU:s medlemsstater. Därtill har Nato ett växande fokus på strategiska cybersäkerhets- och teknikfrågor, och inom Nato bedrivs ett omfattande arbete med cyberförsvar och strategiska tekniker. Den civil-militära kopplingen inom cybersäkerhetsfrågor understryker vikten av ett samordnat utvecklingsarbete mellan Nato och EU inom cybersäkerhet och cyberförsvar.

Det finns vidare internationella konventioner och avtal som i varierande grad ställer krav på och reglerar frågor om cybersäkerhet för Sverige. Omvänt gäller också att Sverige ställer krav på partnerländer. Att folkrätten gäller i cyberrymden har fastslagits i flera rapporter som antagits av FN:s generalförsamling[1]. Inom FN har det dessutom utarbetats icke-bindande normer för ansvarsfullt statligt uppträdande i cyberrymden. Frågor om hur folkrätten ska tillämpas i olika avseenden diskuteras fortsatt bland annat i FN-sammanhang. Sverige publicerade i juli 2022 en nationell position om folkrätten i cyberrymden och EU:s medlemsstater enades i november 2024 om en deklaration om samma fråga.

Svenska flaggan hissas vid Natos högkvarter i Bryssel för att uppmärksamma Sveriges Natomedlemskap.

Foto: Nato

1 Se till exempel resolution A/RES/76/19.

Skyddsrum.

Foto: Niklas Forsström/Regeringskansliet

Cybersäkerhetslandskapet

Sveriges cybersäkerhet påverkas av ett antal sårbarheter som kan ha olika ursprung och manifestera sig inom ett antal områden. Dessa sårbarheter kan samlat eller var för sig utgöra strategiska sårbarheter i ett digitaliserat samhälles cybersäkerhetslandskap och riskera att påverka samhällsviktig verksamhet och ytterst Sveriges säkerhet. Sårbarheter är vanligt förekommande och kan bland annat röra organisatoriska, tekniska, infrastrukturella och mänskliga faktorer.

Sverige står också, likt andra länder, inför en dynamisk och föränderlig hotbild där cyberhotaktörer kontinuerligt utvecklar nya metoder och anammar ny teknik. Såväl att upptäcka sofistikerade cyberangrepp som att definitivt attribuera angrepp till en specifik hotaktör är komplext och bidrar till att cyberangrepp ofta innebär låg risk för påföljder, motåtgärder eller personliga konsekvenser för hotaktörer.

I det följande redogörs dels för ett antal typiska hotaktörer, dels för sårbarheter, som påverkar Sveriges cybersäkerhet. Såväl sårbarheter som antagonistiska hot kan leda till allvarliga konsekvenser. När en incident inträffar kan det också vara svårt att direkt avgöra om skälet är yttre påverkan eller annat fel. Det ska även framhållas att gränsen mellan statliga, kriminella och andra grupperingar ofta är svår att dra. Det finns flera exempel på aktörer inom organiserad brottslighet med nära, men dolda, kopplingar till antagonistiska statliga aktörer.

- Hot från statliga aktörer
- Hot från cyberaktivister
- Hot från cyberbrottslighet och kriminella grupperingar
- Brister i cybersäkerhetsarbetet
- Komplex reglering
- Kompetens- och kunskapsbrist
- Bristande incidenthantering
- Outvecklad informationsdelning mellan den privata och offentliga sektorn
- Sårbara leveranskedjor, beroenden och produkter
- Utmaningar kopplat till utvecklingen i digital infrastruktur och digitala tjänster
- Utmaningar med uppkoppling av enheter och infrastruktur
- Teknikutvecklingen

Hot från statliga aktörer

Cyberangrepp utförda av statliga[1] eller statsunderstödda[2] aktörer mot svenska verksamheter har ökat i omfattning och kan få allvarliga konsekvenser. Statliga aktörer har sofistikerade offensiva cyberförmågor som bland annat kan användas för teknikstöld, underrättelseinhämtning eller annan verksamhet som tillfälligt stör eller förstör hela eller delar av system, ofta inom kritisk infrastruktur och samhällsviktig verksamhet. Cyberangrepp kan frikopplat från, eller inför eller under, en väpnad konflikt komplettera politiska, diplomatiska, ekonomiska, militära och andra medel som en hotaktör nyttjar. Statliga aktörer bedriver också informationspåverkan, bland annat med stöd av cyberangrepp, och nyttjar det fria informationsflödet på internet för antagonistiska syften. Den breda palett av metoder som aktörer använder för att påverka Sverige kan samlas under rubriken hybridhot. Genom sådana hot eftersträvar en motståndare att utnyttja alla sårbarheter i vårt samhälle för att bland annat uppnå sina politiska mål. Cyberangrepp i olika former är en ofta förekommande metod i dessa hybridaktiviteter. God cybersäkerhet försvårar således för hotaktörer att utöva hybridsaktiviteter mot Sverige och svenska intressen.

Hot från cyberaktivister

Cyberaktivister använder cyberangrepp som metod för att främja politiska eller ideologiska syften bland annat genom att exponera eller manipulera data. Cyberaktivister kan, baserat på politiska eller ideologiska motiv, sympatisera med eller agera för olika statsaktörer.

---

1 Statliga aktörer drivs direkt av underrättelse- och säkerhetstjänster eller deras täckföretag alternativt genom organisationer och icke-organiserade individer som agerar ombud.

2 Statliga aktörer kan också understödja kriminella grupperingar baserade i det egna landet eller härrörande från länder som gör lite eller inget alls för att förhindra sådan kriminell verksamhet.

Varvskranarna i Göteborgs hamn.

Foto: Sofia Sabel/Image Bank Sweden

Sjukvård.

Foto: Melker Dahlstrand/Image Bank Sweden

Hot från cyberbrottslighet och kriminella grupperingar

Antalet kriminella grupperingar som ägnar sig åt cyberbrottslighet[1] i form av angrepp på it-system har stadigt ökat. En allt större andel brott begås i digitala miljöer eller med hjälp av digitala verktyg. It-beroende brottslighet kan utgöra hot mot såväl individer, företag och andra organisationer som samhället i stort, där ransomware-angrepp och datastölder är särskilt utmärkande. Denna typ av brottslighet kan få stora konsekvenser för enskilda och leder till stora kostnader för såväl privata som offentliga aktörer. Överbelastningsangrepp utförda av kriminella grupperingar riskerar också att påverka viktiga digitala samhällsfunktioner och förtroendet för dessa funktioner. Både kriminella aktiviteter som initieras av de kriminella grupperingarna själva på eget initiativ och sådana som utförs på uppdrag av någon annan mot betalning,[2] spelar en betydande roll i det it-kriminella ekosystemet.

Cyberbrottslighet är gränsöverskridande och drar nytta av nya verktyg, exempelvis baserade på generativ AI och nya kommunikationstjänster. Information som krävs inom ramen för brottsutredningar finns ofta i andra länder, vilket försvårar brottsbekämpande myndigheters möjligheter till lagföring.

Brister i cybersäkerhetsarbetet

Många organisationer har brister i sitt förebyggande systematiska cybersäkerhetsarbete vilket medför att grundläggande säkerhetsåtgärder inte implementeras. Detta utgör en strategisk sårbarhet. Bland annat små kommuner och mindre aktörer, såsom små och medelstora företag, kan sakna ett tillfredsställande cybersäkerhetsarbete av bland annat resurs- och kompetensskäl. Kunskapsnivån om vad som är skyddsvärt i den egna verksamheten är dessutom ofta låg och många verksamhetsutövare har utmaningar i arbetet med att identifiera vilka delar av verksamheten som är säkerhetskänslig, samhällskritisk eller både och, inte minst ur ett tillgänglighetsperspektiv. Detta gör det svårt att ta medvetna beslut om informationshantering i allmänhet och dimensionering av skyddsåtgärder i synnerhet.

---

1 Cyberbrottslighet kan delas upp i två olika typer: it-beroende (cyber dependent) och it-relaterad (cyber enabled). It-beroende brott är till exempel ransomware och DDoS, medan it-relaterade är traditionella brott som använder sig av it, till exempel bedrägerier och illegal försäljning på nätet.

2 Benämns i vissa sammanhang Crime as a service, CaaS.

Organisationer som saknar tillräckligt förebyggande cybersäkerhetsarbete brister ofta även i analyser över vilka krav deras it-system behöver uppfylla baserat på verksamhetens behov. För att effektivt följa lagkrav och uppnå den förbättring som lagstiftaren avsett, krävs att organisationer genomför en grundlig verksamhetsanalys som komplement. Denna analys kan i sig vara komplex och omfattande, särskilt för organisationer som ansvarar för vitt skilda verksamheter och därmed har olika regleringar och krav att förhålla sig till.

Komplex reglering

Ökad reglering på cybersäkerhetsområdet ställer nya krav på organisationer att hantera cyberrelaterade verksamhetsrisker. Ett systematiskt arbete med cybersäkerhetsrisker stärker vanligen organisationers verksamhet och kan på lång sikt även vara kostnadsbesparande. Samtidigt kan betungande reglering också leda till kostnader för såväl privatpersoner och offentliga aktörer som enskilda näringsidkare. Olika regleringar, såväl nationella som internationella, kan samlat innehålla överlappande krav som är svåra att sortera bland, och som skapar utmaningar i att göra adekvata prioriteringar. Detta är särskilt fallet för mindre aktörer som små och medelstora företag med begränsade resurser. Det statliga cybersäkerhetsarbetet är dessutom uppdelat i olika, delvis överlappande ansvarsområden vilket medför att olika statliga myndigheter ansvarar för tillsyn, föreskrifter och vägledning enligt olika regelverk. Detta riskerar att försvåra för enskilda företag och organisationer att följa reglerna.

Kompetens- och kunskapsbrist

Kompetensförsörjning inom cybersäkerhetsområdet har under en lång tid varit en utmaning. Utöver brister i allmän cybersäkerhetskompetens råder det brist på både cybersäkerhetsexperter och personal med relevant utbildning och arbetslivserfarenhet inom angränsande områden såsom säkerhetsskydd och säkerhet inom så kallad operativ teknik[1], även kallat OT-säkerhet. Denna brist, som även är global, påverkar såväl offentlig som privat sektor. Därtill är den generella kunskapen om cybersäkerhet ofta begränsad hos yrkesroller såsom chefer, jurister, upphandlare och it-utvecklare vilka också sällan arbetar med frågorna. Teknikutveckling och digital omställning bidrar till ett ständigt ökande behov av forskning, kompetens och färdigheter på området. Brist på generell cybersäkerhetskompetens hos organisationer kan dessutom leda till att tydliga krav inte ställs på de för verksamheten viktiga it-systemen. Vidare medför ökad och utvecklad reglering inom cybersäkerhet och säkerhetsskydd samt den återupptagna totalförsvarsplaneringen nya kompetensbehov för både tillsynsmyndigheter och verksamhetsutövare.

Svensk cybersäkerhetsforskning är konkurrenskraftig och det bedrivs framstående forskning vid flera universitet och högskolor. Samtidigt som ett fåtal forskningsområden inom cybersäkerhet är dominerande bedrivs forskning inom andra angelägna cybersäkerhetsfrågor enbart i begränsad omfattning och tvärvetenskapliga perspektiv saknas ofta. Vidare har koordinering inom cybersäkerhetsforskningen i Sverige ofta saknats.

Nyfikna barn.

Foto: Emelie Asplund/Image Bank Sweden

1 Sådana system kan också benämnas cyberfysiska system eller industriella styr- och informationssystem.

Flygstridsledare.

Foto: Besav Mahmod/Försvarsmakten

Bristande incidenthantering

Adekvata arbetssätt för incident- och kontinuitetshantering saknas hos många organisationer och få övar dessa förmågor. Bristande incidenthantering utgör en allvarlig risk för organisationer, särskilt i en tid av ökade cyberhot. Svaga processer ökar organisationers sårbarhet vid cybersäkerhetsincidenter. Bristfällig incidenthantering kan öka risken för förlust av känslig information, förlust av förmågan att tillhandahålla kritiska tjänster och finansiella förluster samt skada förtroendet för en verksamhet.

Cybersäkerhetsincidenter som omfattas av incidentrapporteringskrav ska också rapporteras till behöriga statliga myndigheter, men ett mörkertal i rapporteringen har länge varit en realitet nationellt och internationellt. Detta påverkar möjligheten att skapa en operativ lägesbild och varna andra organisationer, vilket riskerar att förvärra en uppstådd kris. Det minskar också möjligheterna att dra lärdomar och inrikta det förebyggande arbetet.

Mörkertalet i antalet rapporterade cyberbrott försvårar också brottsbekämpande myndigheters förebyggande arbete, operativa hantering och utredning vid cybersäkerhetsincidenter. I förlängningen påverkas möjligheten att lagföra den som har utfört en brottslig handling. Det finns inte någon skyldighet att polisanmäla cyberbrott. Detta ställer krav på skyndsam informationsdelning mellan de myndigheter som tar emot incidentrapportering och brottsbekämpande myndigheter för att öka möjligheten att följa upp brott och att säkra bevis.

Outvecklad informationsdelning mellan den privata och offentliga sektorn

Organisationer är beroende av varandra för att förebygga, uppmärksamma och hantera sårbarheter, hot och cybersäkerhetsincidenter. Privata och offentliga organisationer har tillgång till olika informationsflöden. Expert- och tillsynsmyndigheter tar exempelvis emot incident- och sårbarhetsrapporter, medan privata organisationer innehar majoriteten av samhällets cyberresurser och är centrala för nationell cybersäkerhetsförmåga. Informationsdelning och samarbete mellan och inom privat och offentlig sektor kräver bland annat uppbyggda kommunikationsvägar och adekvata processer samt tillit aktörer emellan. Dessa processer behöver bland annat utgå ifrån och ta hänsyn till privata aktörers affärsintressen och sekretess för affärs- och driftförhållanden. Outvecklat och bristande samarbete mellan det privata och offentliga, nationellt såväl som internationellt, utgör en sårbarhet.

Sårbara leveranskedjor, beroenden och produkter

Incidenter i digitala leveranskedjor, såsom vid systemfel hos leverantörer, kan leda till konsekvenser utanför den organisation som initialt drabbats och kan orsaka störningar i samhällskritiska funktioner. Dagens komplexa beroenden medför dessutom svårigheter att kartlägga sårbarheter i digitala leveranskedjor och försvårar ansvarsutkrävande.

Svag cybersäkerhet hos leverantörer riskerar att påverka säkerheten hos kundorganisationer. Givet att många organisationer är beroende av externt levererade it-driftstjänster, blir organisationer som inte beaktat denna omständighet i sina riskanalyser sårbara om en leverantör misslyckas med att leverera sin tjänst. I sådana fall riskerar organisationen att sakna alternativa lösningar. Det kan vidare innebära allvarliga risker om många organisationer är beroende av samma tjänst eller system.[1] Vid sådan oligopol- eller monopolställning minskas också kundens flexibilitet och valmöjligheter, till exempel möjligheten att nyttja alternativa tjänster vid pågående incidenter. Beroenden av digitala produkt- och tjänsteleveranser från organisationer baserade i tredjeland, kan både vara olämpliga och utgöra en sårbarhet som kan användas som politiskt påtryckningsmedel.

Osäkra digitala produkter med låg cybersäkerhet utgör en stor risk för både nationella och internationella leveranskedjor. Osäkerhet och risker uppstår även ofta vid uppdateringar av hård- och mjukvara. På EU-nivå har detta identifierats som nödvändigt att åtgärda och är i fokus för cyberresiliensförordningen som syftar till att höja tillverkares och leverantörers ansvar för cybersäkerhet och att produkter med digitala element placeras på inre marknaden med färre sårbarheter.[2] Utveckling och bred användning av internationella säkerhetsstandarder på teknik- och cybersäkerhetsområdet kan också bidra till mer robusta leveranskedjor. Utvecklingen av internationella standarder präglas dock i ökad grad av geopolitisk konkurrens.

---

1 Okända brister hos och/eller brister i kravställning mot en it-leverantör som levererar it-stöd till många organisationer riskerar att leda till stora störningar inom såväl privat som offentlig sektor i Sverige. Konsekvensen av att licensavgifter höjs, eller att tjänster upphör, riskerar också bli stora.

2 Den inre marknadens sårbarhet för låg cybersäkerhet är också i fokus för certifieringsramverket som etablerats i cybersäkerhetsakten. Möjligheten att genom certifiering visa uppfyllnad av cybersäkerhetskrav finns reglerat i flera EU-akter såsom NIS 2-direktivet, cyberresiliensförordningen, AI-förordningen och den reviderade eIDAS-förordningen.

Utmaningar kopplat till utvecklingen i digital infrastruktur och digitala tjänster

Sveriges digitala infrastruktur utvecklas kontinuerligt. Nya generationers mobilnät rullas ut och rymden är också en infrastrukturdomän för mobildatakommunikation. Behoven av tillförlitlig och säker digital infrastruktur samt digitala tjänster växer i betydelse och omfattning. Det skapar många nya möjligheter, men ställer också höga krav på både upphandlingsförmåga och en väl utvecklad hantering av sårbarheter och beroenden för såväl privata som offentliga alternativ.

Utmaningar med uppkoppling av enheter och infrastruktur

Processer inom kritisk infrastruktur[1] som tidigare varit manuella eller mekaniska har med tiden digitaliserats alltmer. Denna utveckling förstärks av framväxten av nya så kallade IoT-enheter, som ständigt är uppkopplade, och som kan användas bland annat för att styra och övervaka processer. De system som används inom kritisk infrastruktur har tekniska förutsättningar som särskiljer dem från traditionella it-system och gör dem komplexa att skydda. Säkerhetsarbete inom OT-säkerhet utgör därför en utmaning, bland annat mot bakgrund av kompetensbristerna på området.

IoT-enheter med svag säkerhet kan medföra betydande cybersäkerhetsrisker och kan om de är anslutna till organisationers övriga it-infrastruktur utlösa cybersäkerhetsincidenter. Även för privatpersoner kan IoT-konsumentprodukter med låg säkerhet innebära risker. Sådana produkter kan också nyttjas i botnätverk och användas av hotaktörer för överbelastningsattacker mot andra organisationer.

Teknikutvecklingen

Utveckling av strategiskt viktig teknik skapar möjligheter för Sverige. Teknikutveckling kan påverka samhällets säkerhet. Till exempel kan användning av AI-funktioner effektivisera cybersäkerhetsarbetet. Samtidigt kan AI användas för att genomföra cyberangrepp och desinformationskampanjer med bredare spridning. Cybersäkerhetsincidenter i AI-system får också ökade konsekvenser i takt med att samhällets beroende av sådana system ökar.

Utveckling av kvantteknik och kraftfulla kvantdatorer gör vissa kryptografiska algoritmer alltmer sårbara för forcering. Genom bland annat cyberangrepp, avlyssning och annan underrättelseinhämtning kan kvalificerade hotaktörer få tillgång till krypterade data som de lagrar i syfte att kunna forcera när kvanttekniken i framtiden utvecklats.

1 Kritisk infrastruktur innefattar bland annat tjänster och tillhandahållare av dessa inom sektorerna finans, transport, energi och elektronisk kommunikation. Det kan också handla om it-infrastruktur som används brett inom statlig och kommunal förvaltning. Denna uppräkning ska dock inte ses som uttömmande eller som en legal definition. Kritisk infrastruktur innefattar en mängd verksamheter, varav många omfattas av NIS 2-direktivet, säkerhetsskyddsregleringen eller andra sektorsspecifika unionsrättsakter som innehåller motsvarande cybersäkerhetskrav såsom DORA-förordningen.

Max IV-laboratoriet i Lund.

Foto: Per Pixel Petersson/Image Bank Sweden

Regeringens inriktning

Strategin utgår från tre pelare som anger inriktning för Sveriges cybersäkerhetsarbete.

Pelarna innehåller i sin tur ett antal mål med tillhörande resultatindikatorer. Strategins mål tar sikte på ett antal områden för att åstadkomma förflyttningar och bemöta de hot och sårbarheter som beskrivs i avsnittet Cybersäkerhetslandskapet. Målen i strategin sträcker sig till och med 2029. För respektive mål finns en inledning som beskriver målet och sätter det i sitt sammanhang. Därefter presenteras under rubriken 'Önskat läge 2030' regeringens vision för var Sverige befinner sig, och vilka förflyttningar som skett, inom respektive mål vid strategins utgång. Givet det långsiktiga utvecklingsarbetet med NCSC, där centret ska vara navet för det nationella cybersäkerhetsarbetet, ser regeringen att centret har en väsentlig roll inom ett flertal av målområdena och uppföljning av dessa.

Till strategins pelare och mål kopplas en handlingsplan (bilaga 1) med ett antal aktiviteter som svarar mot regeringens inriktning och kraven i NIS 2-direktivet. Handlingsplanens innehåll kommer att uppdateras löpande och aktiviteter tillföras för att stegvis uppnå målen.

Pelare A: Systematiskt och effektivt cybersäkerhetsarbete

Pelare B: Utvecklad kunskap och kompetensutveckling inom cybersäkerhet

Pelare C: Förmåga att förhindra och hantera cybersäkerhetsincidenter

Pelare A: Systematiskt och effektivt cybersäkerhetsarbete

handlar om att öka svensk motståndskraft genom att ge förutsättningar för alla samhällets organisationer att stärka sitt systematiska cybersäkerhetsarbete, om att öka säkerheten i digitala leveranskedjor och produkter, och om att skydda kritiska system och verksamheter.

Utöver aktiviteterna i handlingsplanen gäller följande övergripande resultatindikatorer för pelare A:

- Antalet organisationer som nyttjat NCSC:s råd och stöd inom cybersäkerhetsområdet har ökat.
- Antalet statliga myndigheter som genomfört cybersäkerhetsmätningar har ökat.
- Andelen organisationer som genom systematiska arbetssätt implementerat cybersäkerhetsåtgärder, både administrativa och tekniska, har ökat.

Mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer

Ett robust samhälle har behov av väl fungerande it-system varför grundläggande cybersäkerhetsarbete skapar förutsättningar för att hantera fredstida kriser och ytterst krig. I ett digitaliserat samhälle behöver därför alla organisationer ha ett fullgott, systematiskt säkerhetsarbete och som en del av detta implementera cybersäkerhetsåtgärder. Respektive organisations ledning har det yttersta ansvaret för sin verksamhet och därmed dess cybersäkerhet. Kraven i NIS 2-direktivet på att ledningsorgan ska godkänna riskhanteringsåtgärder för cybersäkerhet och övervaka deras genomförande samt genomgå utbildning lägger en god grund, men måste i sin tur baseras på en grundläggande förståelse för hur verksamheten kan påverkas av en cyberrelaterad incident.

Önskat läge 2030

Organisationer som bedriver samhällsviktig verksamhet genomför noggranna verksamhetsanalyser för att identifiera vilken cybersäkerhetsförmåga som är nödvändig för att garantera organisationens verksamhet. Berörda statliga myndigheter har genom aktivt deltagande i EU-samarbetet kring NIS 2-direktivets krav tagit fram nationellt anpassade vägledningar och stöd. Tillsammans med relevanta standarder stöttar berörda statliga myndigheters vägledning organisationers anpassning till NIS 2-direktivets krav och därigenom införandet av proportionella säkerhetsåtgärder. NIS 2-direktivets kravnivå får genomslag även hos organisationer som inte omfattas av direktivet, särskilt organisationer med samhällskritisk funktion som redan omfattas av reglering med omfattande krav men som saknar allriskperspektiv. Sektorsspecifika cybersäkerhetsakter, som till exempel DORA-förordningen, tillämpas och utvidgar kraven på motståndskraft till ytterligare aktörer. En grundläggande cyberhygien är en integrerad del i all samhällsviktig verksamhet och en ökad cybersäkerhetsmognad inom alla samhällskritiska sektorer är uppnådd. Offentliga aktörer och företag, oavsett storlek, arbetar aktivt med kontinuitetsplanering som en central del av sin beredskap.

Alla organisationer har förutsättningar för och tar ansvar för att skydda sin information och de nätverks- och informationssystem som används för verksamheten eller för att tillhandahålla tjänster. Även tillgång till information samt till funktioner och förmågor upprätthålls. Skyddet dimensioneras utifrån såväl verksamhetens och informationens säkerhetsbehov som reglerade krav och stöttas av välutvecklat stöd och vägledning från de statliga myndigheter som har i uppgift att ge sådant stöd. Organisationer har en planering för vilken verksamhet som alltid behöver kunna upprätthållas vid störningar eller incidenter. Privat-offentlig samverkan har utvecklats inom flera sektorer för att spegla privata aktörers alltmer centrala ställning för nationell säkerhet. Berörda statliga myndigheter erbjuder utbildning till ledningsorgan inom samhällsviktig verksamhet och beredskapsorganisationer.

En gemensam och dimensionerad nationell cybersäkerhet som bygger på reglerad kravställning, fastställda säkerhetsnivåer och nationellt kravställda produkter och tekniska lösningar har implementerats i skyddsvärda verksamheter såväl offentligt som privat.

Kraftledningar i vinterfrost.

Foto: Tomas Arlemo/Svenska kraftnät

Mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering

Att den offentliga sektorn kan säkerställa en hög nivå av cybersäkerhet är avgörande för att upprätthålla ett högt förtroende för offentliga institutioner. Statliga myndigheters, kommuners och regioners förutsättningar och resurser att bedriva ett fullgott cybersäkerhetsarbete skiljer sig samtidigt åt. Rysslands fullskaliga invasion av Ukraina har också aktualiserat frågan om statens förmåga att upprätthålla samhällsviktiga tjänster och kritisk infrastruktur samt skydda viktiga grunddata även i kris och ytterst krig.

Önskat läge 2030

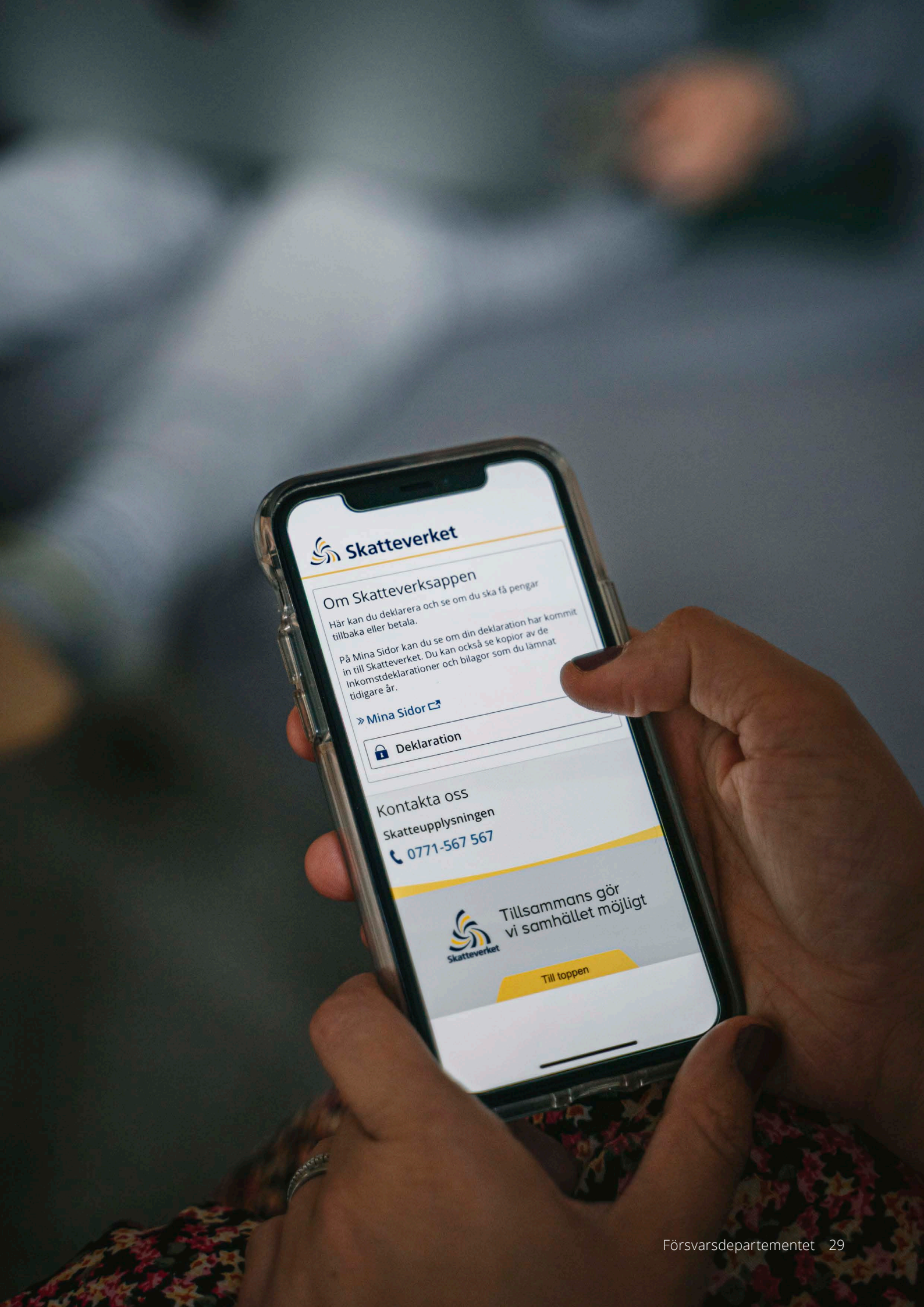
Berörda statliga myndigheters verktyg för cybersäkerhetsmätningar utvecklas och får större genomslag i att stödja andra organisationer med att kartlägga det interna cybersäkerhetsarbetet. Tillhörande råd om vilka åtgärder som organisationer, utifrån deras resultat i cybersäkerhetsmätningar, bör vidta har utvecklats och fått större genomslag. Kraven i den svenska reglering som genomfört NIS 2-direktivet har lagt en god grund för att höja cybersäkerheten i den offentliga förvaltningen vilket också framgår i förmågebedömningar av aktörernas cybersäkerhet inom det civila försvaret. Enhetliga säkerhetskrav och säkerhetsnivåer i den offentliga sektorn främjar upprätthållandet av cybersäkerhet i hela hanteringskedjan och en gemensam stark cybersäkerhet.

Statliga myndigheter erbjuder samordnade, säkra och i möjligaste mån kostnadseffektiva alternativ för gemensam digital infrastruktur och it-tjänster, vilket har underlättat för aktörer med bristande cybersäkerhetsförmåga och bidragit till att säkerställa samhällsfunktioner genom hela konfliktskalan. Ramavtal finns på plats med cybersäkerhetskrav som skyddar konfidentialitet, riktighet och tillgänglighet. Upphandling med adekvata krav resulterar i avtal med robusta säkerhetskrav som leder till väl fungerande tjänster, säker hantering av information, samt innovation inom säkerhetsområdet. Sammantaget tryggas samhällets tilltro till att rätt information alltid finns tillgänglig för rätt part.

Statliga myndigheters nationella insatser kring tekniskt stöd är kostnadseffektiva och möter målgruppens behov. Fler kollektiva tekniska säkerhetslösningar erbjuds centralt och stöttar särskilt cybersäkerheten hos små organisationer i myndighetssektorerna och i kommuner och regioner där information som är av betydelse för samhällskritisk och samhällsviktig verksamhet återfinns. Kommuner och regioner har identifierat och implementerat fler effektiva gemensamma metoder för att höja sin kollektiva cybersäkerhet.

Digitala samhällsviktiga tjänster.

Foto: Liselotte van der Meijs/Image Bank Sweden


Skatteverket
Om Skatteverksappen
Här kan du deklarera och se om du ska få pengar tillbaka eller betala.
På Mina Sidor kan du se om din deklaration har kommit in till Skatteverket. Du kan också se kopior av de inkomstdeklarationer och bilagor som du lämnat tidigare år.
» Mina Sidor
Deklaration
Kontakta oss
Skatteupplysningen
0771-567 567
Skatteverket
Tillsammans gör vi samhället möjligt
Till toppen


Kritisk infrastruktur
Annan samhällsviktig verksamhet
Samhället i övrigt

Mål 3: Stärkt cybersäkerhetsarbete inom kritisk infrastruktur

Att kritisk infrastruktur kan upprätthållas är nödvändigt för samhällets säkerhet och stabilitet. Många av de tjänster och funktioner som utgör kritisk infrastruktur tillhandahålls av privata organisationer. Cybersäkerhetsarbetet för operatörer av kritisk infrastruktur behöver bland annat därför utgå från verksamheternas individuella förutsättningar, men också från deras särskilda sårbarheter och den specifika hotbild som riktas mot den aktuella verksamheten. Samhällets beroende av dessa verksamheter gör deras cybersäkerhetsarbete centralt. Stärkt cybersäkerhetsarbete bidrar också till att försvåra för hotaktörer att rikta cyberattacker mot kritisk infrastruktur som en del av hybridaktiviteter för att påverka Sverige.

Önskat läge 2030

Operatörers skydd av kritisk infrastruktur, inklusive säkerhetsarbetet inom OT, dimensioneras utifrån infrastrukturens samhällsbetydelse och antagonistiska hotbild. Säkerhetsövervakning av it- och OT-system inom kritisk infrastruktur stimuleras. Sektorsansvariga myndigheter enligt NIS 2-regelverket samt andra berörda statliga myndigheter nyttjar NCSC:s råd och stöd inom cybersäkerhet för att sektorsanpassa vägledningar och andra styrdokument för respektive sektor. Operatörers arbete med att implementera säkerhetsåtgärder stärks därigenom vilket, tillsammans med deras hantering av sårbarheter, leder till höjd motståndskraft. Statliga myndigheter utvecklar stöd för skydd av kritisk infrastruktur. NIS 2- och beredskapsorganisationer tillgodogör sig det stöd och den utbildning som erbjuds inom säkerhet för kritisk infrastruktur. Samarbetet och informationsdelningen mellan statliga myndigheter och operatörer av kritiska system har utvecklats och sammanlänkar sektorer, utifrån att sektorer ofta har tydliga överlapp och beroenden sinsemellan. Övnings- och testverksamhet som möjliggörs genom bland annat cyber range-miljöer fortsätter utvecklas och nyttjas i bred utsträckning. Sektorsspecifika samarbetsforum har fortsatt en central roll när det gäller samverkan, övningsverksamhet och informationsdelning, och ett ökat samarbete sker mellan statliga myndigheter och näringslivet.

Reningsverk.

Foto: Per Pixel Petersson/Image Bank Sweden

Mål 4: Robustare digitala leveranskedjor och minskat beroende

Hantering av digitala leveranskedjor, molntjänster och beroenden utgör en central prioritering för regeringens cybersäkerhetsarbete. För att stärka Sveriges cybersäkerhet behöver monoberoenden och kritiska tredjelandsberoenden identifieras och hanteras och digitala leveranskedjor bli mer robusta.

Önskat läge 2030

Sverige har en hög ambition i det nationella och det internationella arbetet för säkerhet i digitala leveranskedjor, särskilt på EU-nivå. Statliga myndigheter ger organisationer, såväl privata som offentliga, vägledning när det gäller inventering av leveranskedjor och utkontraktering. Organisationer inventerar och bedömer säkerheten i sina leveranskedjor samt ställer adekvata cybersäkerhetskrav i avtal med leverantörer. Även de organisationer som inte omfattas av NIS 2-direktivet bedömer beroenden och risker i sina leveranskedjor samt säkerställer nödvändiga reservrutiner.

Bestämmelserna i cyberresiliensförordningen om cybersäkerhet i produkter med digitala element leder till ökad säkerhet i leveranskedjor. Svenska företag som tillämpar säker utveckling av mjukvara och fast programvara samt inbyggd säkerhet är mer konkurrenskraftiga och bidrar till att förse marknaden med produkter med färre säkerhetsbrister. Efterfrågan på säkra produkter bland organisationer i Sverige har ökat, pådrivet av högre och bättre kravställning från den offentliga sektorn när det gäller tjänster och produkters funktion. Sverige slår vakt om fortsatt inflytande inom internationell standardisering och bidrar till välanpassade internationella standarder som främjar säkra leveranskedjor. 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. Organisationer nyttjar cybersäkerhetscertifierade it-tjänster och produkter utifrån sin riskbedömning.

Ambulanspersonal.

Foto: Helena Wahlman/Image Bank Sweden

Mål 5: Förenklad regelefterlevnad och stärkt funktionellt tillsynsarbete

Regleringen på området kommer kontinuerligt att öka och i takt med växande systemintegration, där fler aktörer blir beroende av varandra, är ytterligare reglering och skärpta cybersäkerhetskrav för fler aktörer att vänta. För att höja samhällets cybersäkerhet, är det därför viktigt att så långt som möjligt förenkla organisationers tillämpning av komplexa regler samt att stärka och samordna tillsynsmyndigheters verksamhet. Förenklad regelefterlevnad kan också stärka konkurrenskraften hos företag.

Önskat läge 2030

Sverige är, med stöd i genomförda nationella åtgärder, en ledande medlemsstat i utvecklingen av nya internationella regelverk inom cybersäkerhet som innehåller proportionerliga och harmoniserade regler. Statliga myndigheters aktiva deltagande i erfarenhetsutbytet på EU-nivå bidrar till harmoniserade NIS 2-krav mellan medlemsstater. NIS 2-direktivets krav har omsatts i ensade regelverk sektorerna emellan och skapat förutsättningar för effektiv regelefterlevnad. Statliga myndigheter är väl koordinerande när det gäller befintlig reglering i syfte att föreskrifter, allmänna råd och vägledningar så långt som möjligt ensas och följer en likartad logik, struktur och terminologi. NCSC:s råd och stöd i cybersäkerhetsfrågor kompletterar sektorsmyndigheternas föreskriftsarbete. Genom kontinuerligt utvecklad tillsynsverksamhet stärks efterlevnaden av cybersäkerhetsregleringen. Myndigheter med centrala roller har rätt befogenheter och mandat.

Mål 6: Utvecklat stöd för små och medelstora företags cybersäkerhetsarbete

Näringslivet står för stora ekonomiska värden kopplat till såväl innovation som produktion och samhällsviktiga tjänster. Små och medelstora företag utgör majoriteten av företagen i Sverige och står sammantaget för en ansenlig del av dessa värden, samtidigt som de generellt sett är mer sårbara än större företag för cybersäkerhetsrisker. När dessa drabbas av cybersäkerhetsincidenter kan omfattande produktionsbortfall, störningar i samhällsviktiga tjänster och ekonomiska konsekvenser uppstå. Vissa små och medelstora företag har god cybersäkerhet, och det finns även ett starkt segment av sådana bolag verksamma inom cybersäkerhetsfältet, men faktorer som bristande cybersäkerhetsmedvetenhet och knappa resurser gör majoriteten av dem sårbara. Dessa löper dessutom ofta stor risk att inte återhämta sig från allvarliga cybersäkerhetsincidenter. Små och medelstora företags motståndskraft och skydd av affärshemligheter är därför en väsentlig del i att slå vakt om Sveriges samlade konkurrens- och motståndskraft.

Önskat läge 2030

Statliga myndigheter erbjuder i större utsträckning stöd och vägledning som stöttar små och medelstora företag, även till dem som inte omfattas av den svenska reglering som genomfört NIS 2-direktivet. Statliga myndigheters samarbeten med intresse- och företagsorganisationer stimuleras och nyttjas för att motverka digitala brott och öka cybersäkerheten. Teknikföretag tar ansvar för att erbjuda säkra tjänster, vilket indirekt stärker små och medelstora företags cybersäkerhet genom säkrare it-tjänster. Små och medelstora företag nyttjar stöd som erbjuds av organisationer såsom regionala handelskammare och bransch- och intresseorganisationer. Därtill ser aktörerna tillsammans över möjligheterna att nyttja gemensamma tekniska säkerhetslösningar vilket minskar små och medelstora företags behov att med egna resurser och kompetens omhänderta väsentliga områden för att cybersäkra sin verksamhet. EU:s kompetenscentrum för cybersäkerhet nyttjas genom att små och medelstora företag, via det nationella samordningscentret (NCC-SE), kan ansöka om medel för stärkt cybersäkerhetskapacitet.

Lindholmen Science Park.

Foto: Lindholmen Science Park

Pelare B: Utvecklad kunskap och kompetensutveckling inom cybersäkerhet

Utvecklad kunskap och kompetens inom cybersäkerhet handlar om att öka medvetenheten, utveckla och bygga kompetens inom cybersäkerhet på alla nivåer samt att främja svensk forskning, innovation och säker tillämpning av ny teknik.

Utöver aktiviteterna i handlingsplanen gäller följande övergripande resultatindikatorer för pelare B:

- Andelen personer som har nåtts, och tagit till sig av, informationskampanjer om cybersäkerhet har ökat.
- Antalet forsknings- och innovationsprojekt inom cybersäkerhet som har fått EU-finansiering har ökat.
- Antalet företag verksamma inom cybersäkerhet i Sverige har ökat.
- Antalet utbildade inom cybersäkerhet eller motsvarande har ökat.
- Antalet företag som genomgått verksamhetscertifiering inom cybersäkerhet har ökat.

Mål 7: Ökad cybersäkerhetsmedvetenhet och cyberhygien i samhället

En tilltagande exponering för digitala hot och risker ställer krav på god cyberhygien och en medveten säkerhetskultur i hela samhället. Med cyberhygien avses grundläggande åtgärder för att skydda sig själv och andra online. Säkrare internetanvändning hos den enskilde bidrar till att Sveriges cybersäkerhet stärks genom att sårbarheten för bedrägerier och cyberangrepp minskar. Att åstadkomma beteendeförändringar hos allmänheten kräver kontinuerliga insatser från olika organisationer, såväl privata som offentliga och ideella.

Önskat läge 2030

Medborgare är välinformerade om vikten av god cyberhygien och är bättre rustade för att hantera och möta cybersäkerhetsrisker. Åtgärder genomförs för att ge individer, utifrån deras förutsättningar och behov, bättre möjligheter till god cyberhygien. Arbetsgivare säkerställer också att processer och rutiner främjar säkra arbetssätt och cybersäkerhetsmedvetenhet. Statliga myndigheters informations- och utbildningskampanjer utvecklas löpande i syfte att få större genomslag och för att främja beteendeförändringar i samhället. Statliga myndigheter, ideella organisationer och företag bedriver i samarbete informations- och utbildningsinsatser inom cybersäkerhet för allmänheten. I detta beaktas skillnader i utsatthet för cybersäkerhetsrisker och skillnader i grundförutsättningar till god cyberhygien. Arbetet med att höja cybersäkerhetsmedvetenheten går hand i hand med insatser för att motstå hybridaktiviteter såsom stöd till medie- och informationskunnighet, bemötandet av desinformationskampanjer och Sveriges deltagande i det internationella arbetet med att stärka normer och regler för att värna det fria digitala informationsflödet. Exponering och ansvarsutkrävande av statliga cyberhotaktörer, inklusive inom utrikes- och säkerhetspolitiken, bidrar också till cybersäkerhetsmedvetenhet.

Kontor.

Foto: Niklas Forsström/Regeringskansliet

Mål 8: Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet

Kompetens inom cybersäkerhet blir allt viktigare och efterfrågan har länge varit större än utbudet. Utbildningsväsendet har en central roll i att möta samhällets behov genom att tillgodose grundläggande kunskaper i ämnet, väcka och stimulera intresse och ytterst stärka kompetensförsörjningen inom cybersäkerhet. Därtill behöver cybersäkerhetskompetensen hos arbetsgivare och arbetstagare stärkas för att möta dagens och morgondagens behov inom cybersäkerhet. Befintlig kompetens behöver utvecklas och ny arbetskraft attraheras.

Önskat läge 2030

Mer tillämpbara kunskaper i cybersäkerhet får genomslag i utbildningen i grundskolan, anpassade grundskolan, specialskolan och sameskolan. Elever i gymnasieskola, anpassad gymnasieskola och kommunal vuxenutbildning ges förutsättningar att förstå vikten av samhällets cybersäkerhet samt att få praktiska cybersäkerhetsfärdigheter. Både privata och offentliga organisationer bidrar fortsatt med interaktiva utbildningspaket och moduler som kan nyttjas för utbildning och fortbildning inom cybersäkerhet. Högskolor, universitet och yrkeshögskolor överväger om och hur cybersäkerhet bör införas i utbildningar. Därmed blir cybersäkerhet alltmer sammankopplat med alla ämnesområden.

Grundläggande och förutsättningsskapande utbildning för cybersäkerhet, såsom matematik, datavetenskap och kryptologi, står sig fortsatt stark. Interaktiva spel och tävlingar som vänder sig till ungdomar för att stimulera och väcka intresse för praktisk cybersäkerhet har bred spridning.

Cybercampus Sverige utgör ett nav för utbildning inom området och bidrar till förstärkt kompetensförsörjning av cybersäkerhetsexperter inom både offentlig och privat sektor. Organisationer såsom lärosäten, andra myndigheter och utbildningsanordnare inom yrkeshögskolan har tecknat avsiktsförklaringar att ingå i Cybercampus inom ramen för verksamheten.

Statliga myndigheter verkar fortsatt för att väcka intresse för arbete inom cybersäkerhet. Berörda statliga myndigheter, kommuner och regioner samt andra organisationer har ett aktivt branschsamarbete om kompetensförsörjning inom cybersäkerhetsområdet och sprider kunskap om arbetsgivarnas nuvarande och framtida kompetensbehov. Nya målgrupper övervägs i större utsträckning för roller där avsaknad av tidigare erfarenhet eller utbildning inom området kan tillgodoses genom intensiv- och internutbildningar. Livslångt lärande och karriärbyte främjas, med omställningsstudiestödet eller liknande som en möjliggörare. Arbetsgivare säkerställer god fortbildning för anställda som arbetar med cybersäkerhet men också kompetensutveckling för andra medarbetare, chefer och ledning kring cybersäkerhet. Statliga myndigheter och privata organisationer erbjuder trainee-program inom cybersäkerhet i privat-offentlig samverkan. Därtill inspireras organisationer av, och utvärderar hur, lyckade satsningar i andra länder som rör kunskaps- och erfarenhetsutbyten kan omsättas till en svensk kontext.

Universitetsutbildning.

Foto: Magnus Liam Karlsson/Image Bank Sweden


VGGOPAENQÖFDFWNÄ
BZMMRTXHJFVAEKEA
MVOALPÄWARRBÖYPU
HDNTTÅSAFSSJÖEDI
SIAWQGECXMÖKDAFA
GADÄYBACKASXWOMA
NRBFZÅISREEMVDCC
RHJJBZKAAGHRCEPÄ
BEHSMDAMEGQLMFQL
LTYVBCKLACMSNKFR
IOHEHAPÅLWKVOHDA
TJEGIBJKECHFLBMZ
CURWAMANFUIMCLJX
FDGVITODDJRAWNTR
HVAFAJYÅMVVLOVEK
FANTOMENFBRCOBTM
TJAGAVVTTDRTTKTA
HJBAJKNTKOLTLYRP
YYTTRAQLAGARYIPÄ
TBMRCTEGFTMTBGRY
OÅWBVCGDDHFENDTM
BHREANNMARKANVKA
ÖVARPQRBVGGMYTRA

Mål 9: Stärkt forskning och innovation på cybersäkerhetsområdet

I Sverige finns många världsledande teknikföretag, inklusive en expansiv cybersäkerhetsindustri innehållandes många innovativa små och medelstora företag som utvecklar och erbjuder konkurrenskraftiga cybersäkerhetslösningar. Traditionen av nära samarbete mellan staten, lärosäten och industri finns även inom cybersäkerhetsområdet. Cybersäkerhetsforskning bedrivs vid flertalet universitet och högskolor vilka finansieras av såväl statliga som privata forskningsfinansiärer. Sverige har starka forskargrupper inom vissa av cybersäkerhetsforskningens områden men fältet är splittrat. En viktig faktor är att organisationer och företag ges goda förutsättningar för innovation, forskning och investeringar inom cybersäkerhetsområdet i Sverige. Nyttjandet av möjligheter och finansiering från bland annat EU:s program och fonder behöver öka.

Önskat läge 2030

Sveriges forsknings- och teknikintensiva näringsliv inom cybersäkerhetsområdet ligger fortsatt i framkant och konkurrerar på en global marknad. Regeringens kraftfulla satsningar på forskning och innovation för banbrytande och strategisk teknik i den forsknings- och innovationspolitiska propositionen Forskning och innovation för framtid, nyfikenhet och nytta (prop. 2024/25:60) har även skapat goda förutsättningar för stärkt cybersäkerhetsforskning.

Satsningar som Cybercampus Sverige har stärkt forskning och innovation inom cybersäkerhet och bidrar till ett säkert digitaliserat och motståndskraftigt Sverige. Genom god samverkan med och mellan lärosäten och näringsliv fortsätter utvecklingen av funktioner såsom Cybercampus, Cybernoden och NCC-SE. Utvecklingen bidrar till ökad koordinering av cybersäkerhetsforskning och innovation samt goda förutsättningar för entreprenörskap på området. Forskning och innovation på cyberområdet har även en tvärvetenskaplig ansats och kommer därmed hela samhället till del genom att teknisk expertis alltmer sammanlänkas med andra ämnesområden. Forskningsresultat inom området leder i större utsträckning till innovation och kommersialisering. Statliga myndigheter bidrar aktivt till utveckling och kommersialisering av cybersäkerhetsinnovation genom exempelvis innovationsdrivande upphandling och stöttar organisationer att nyttja finansieringsmöjligheter för cybersäkerhet inom EU. Det finns en tillräckligt hög nivå av nationell medfinansiering för att säkra svenska aktörers aktiva och långsiktiga medverkan i fonder och program exempelvis inom cybersäkerhetsområdet. Sverige påverkar på ett tidigt stadium innehåll i arbetsprogram inför kommande utlysningar. Internationella forsknings- och innovationssamarbeten kring cybersäkerhet har ökat inom såväl EU och Nato som bilateralt med likasinnade länder.

Mål 10: Stärkt förmåga att hantera framväxande teknologiers risker och möjligheter

Utvecklingen inom framväxande, banbrytande och strategiskt viktiga tekniker går snabbt. AI och kvantteknik är exempel på områden där omfattande framsteg har skett med relevans för cybersäkerhetsområdet. Ökad förmåga att hantera framväxande teknologier stärker både nationell säkerhet och konkurrenskraft. För att möta risker och möjligheter med framväxande teknologier behöver berörda organisationer prioritera arbetet, och det är centralt med innovation och forskning av hög kvalitet inom teknikområden.

Utvecklingen inom kvantteknik, framför allt kvantdatorer, påverkar kryptografiska tekniker, vilket är ett väsentligt säkerhetsintresse och ett område där Sverige traditionellt legat i framkant. Organisationer har goda förutsättningar att skydda säkerhetsskyddsklassificerade uppgifter genom tillgång till godkända kryptografiska system som redan är kvantdatorsäkra, men fler insatser krävs för att bibehålla och utveckla förmågan samt för att kvantsäkra information som inte är säkerhetsskyddsklassificerad.

Teknikutveckling i stort, och kanske särskilt AI-utvecklingen, är ur många perspektiv fördelaktig men medför också ytterligare krav på cybersäkerhetsarbetet och på kontinuerlig utveckling av regelverk för att möta både möjligheter och utmaningar. Utvecklingen och implementeringen av säkra och etiska AI-system blir allt viktigare.

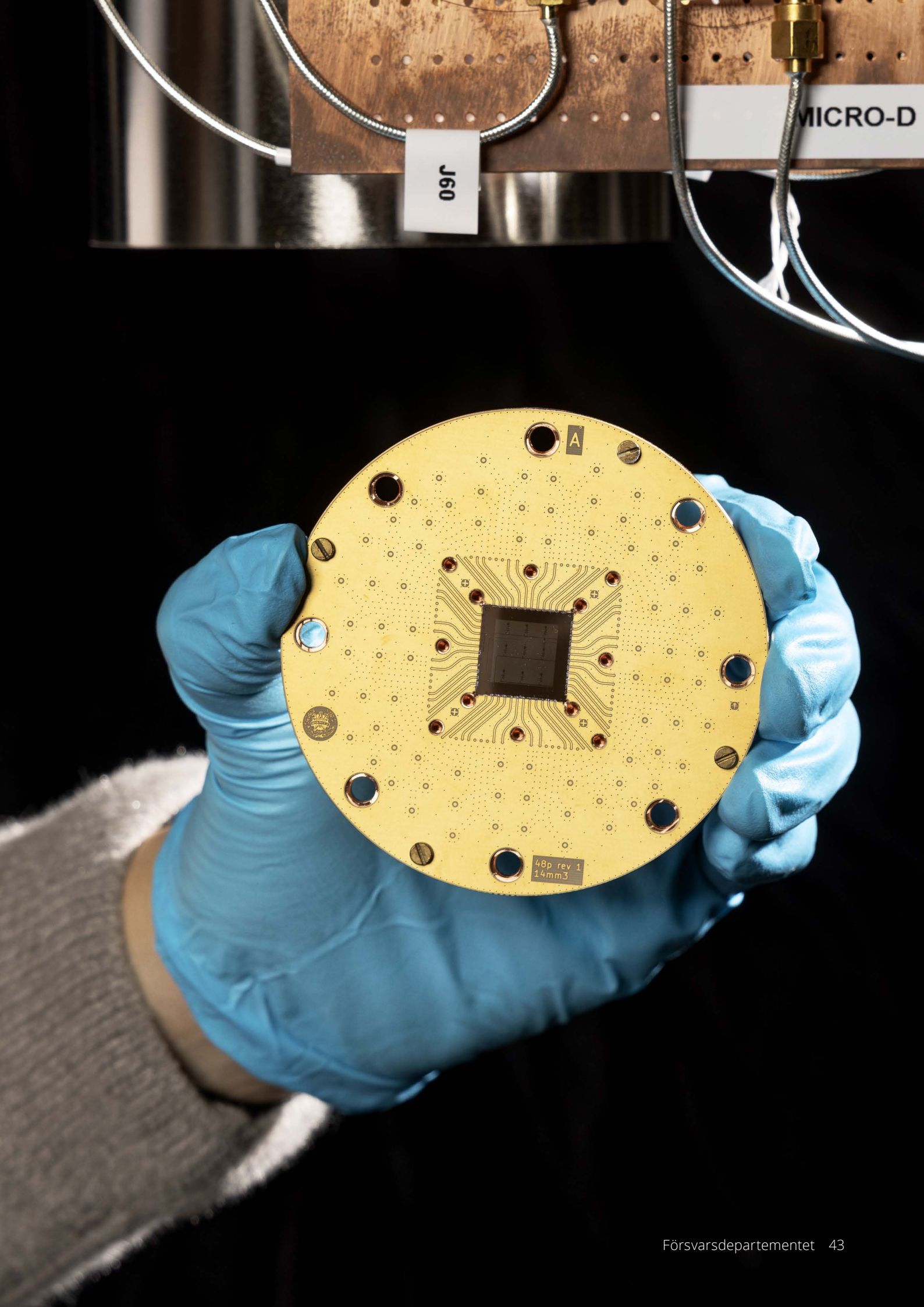
Önskat läge 2030

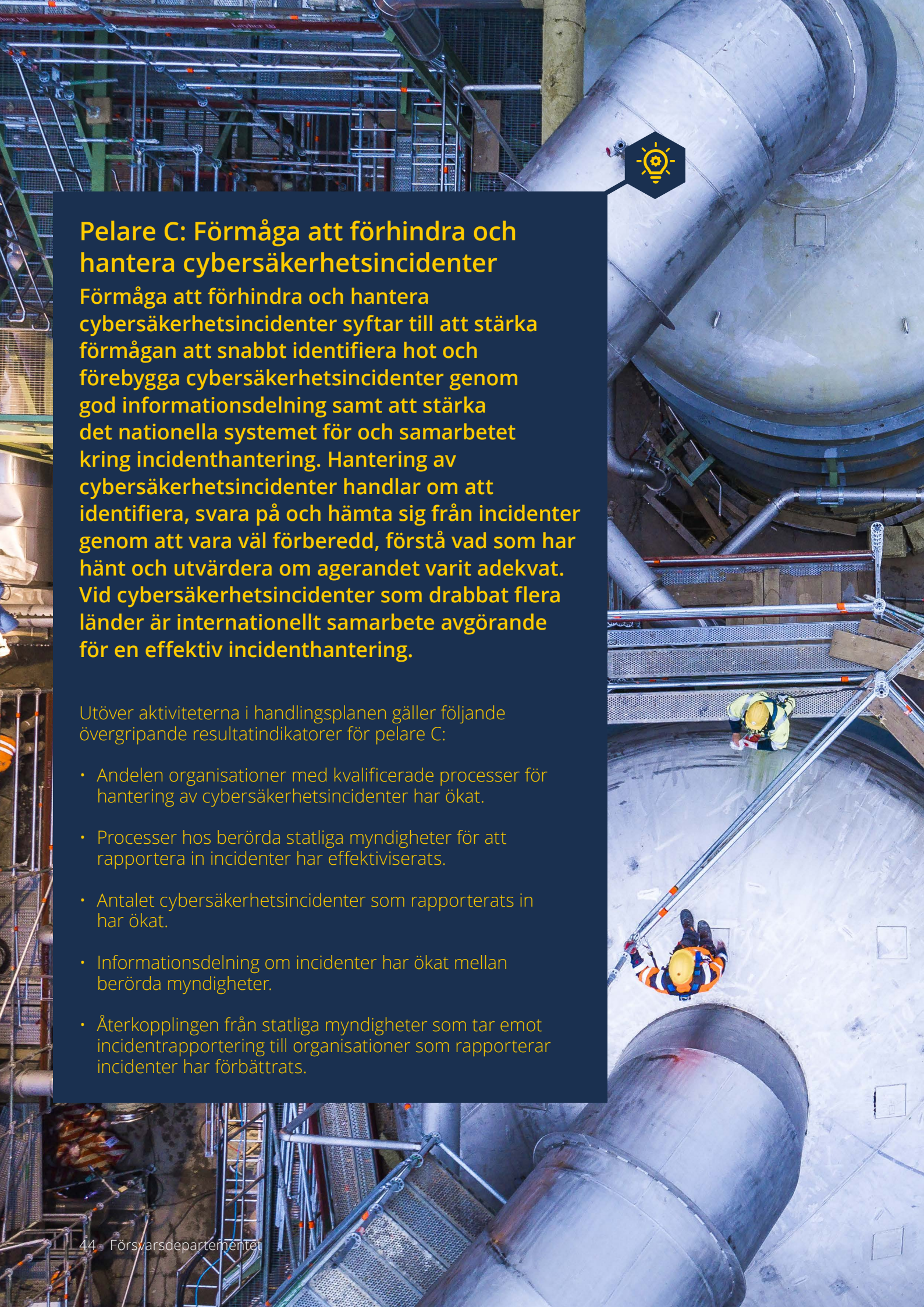
Utvecklingen av AI nyttjas till en omfattande positiv påverkan på cybersäkerhetsområdet. Sverige har god tillgång till kompetens inom AI och är representerat i de internationella sammanhang där utveckling sker och kan därmed identifiera och hantera risker med AI, men också dra nytta av de möjligheter som AI innebär för cybersäkerhet.

Statliga myndigheter bibehåller en hög grad av kompetens, självförsörjning och nationellt oberoende i fråga om signalskydd. Utifrån antagandet om att kryptografiskt relevanta kvantdatorer kan komma att vara i bruk från början av 2030-talet, utvecklas och införs kvantsäkra kryptografiska funktioner i linje med de behov av koordinering och standardisering som följer av Sveriges EU- och Natomedlemskap. Kvantdatorsäkra kryptografiska lösningar prioriteras även för information som är känslig men inte säkerhetsskyddsklassificerad, såsom vissa affärshemligheter och personuppgifter. Berörda statliga myndigheter verkar för att kritiska krypteringstekniker och produkter även fortsättningsvis utvecklas i Sverige och anpassas för såväl nationella behov som behov inom EU och Nato. Svensk kryptoindustri och nya svenska företag på området har möjligheter att utvecklas i Sverige och leverera på en internationell marknad. Statliga myndigheter bidrar fortsatt till arbetet med kryptografiskt skydd inom EU och arbetet med att utveckla ett aktivt bidrag till Natos förmåga inom området, bland annat genom att skapa förutsättningar för att svenska kryptografiska produkter ska kunna användas inom alliansen. Regeringens kraftfulla satsningar på forskning och innovation för banbrytande och strategisk teknik i den forsknings- och innovationspolitiska propositionen Forskning och innovation för framtid, nyfikenhet och nytta (prop. 2024/25:60) har ökat den långsiktiga kompetensförsörjningen inom olika teknikområden, vilket är av stor betydelse för såväl svensk konkurrenskraft och samhällsutveckling som cybersäkerhet.

Chip till kvantdator.

Foto: Sofia Sabel/Image Bank Sweden


J60
MICRO-D
A
48p rev 1
14mm3



Pelare C: Förmåga att förhindra och hantera cybersäkerhetsincidenter

Förmåga att förhindra och hantera cybersäkerhetsincidenter syftar till att stärka förmågan att snabbt identifiera hot och förebygga cybersäkerhetsincidenter genom god informationsdelning samt att stärka det nationella systemet för och samarbetet kring incidenthantering. Hantering av cybersäkerhetsincidenter handlar om att identifiera, svara på och hämta sig från incidenter genom att vara väl förberedd, förstå vad som har hänt och utvärdera om agerandet varit adekvat. Vid cybersäkerhetsincidenter som drabbat flera länder är internationellt samarbete avgörande för en effektiv incidenthantering.

Utöver aktiviteterna i handlingsplanen gäller följande övergripande resultatindikatorer för pelare C:

- Andelen organisationer med kvalificerade processer för hantering av cybersäkerhetsincidenter har ökat.
- Processer hos berörda statliga myndigheter för att rapportera in incidenter har effektiviserats.
- Antalet cybersäkerhetsincidenter som rapporterats in har ökat.
- Informationsdelning om incidenter har ökat mellan berörda myndigheter.
- Återkopplingen från statliga myndigheter som tar emot incidentrapportering till organisationer som rapporterar incidenter har förbättrats.

Mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt

Att kontinuerligt kartlägga, identifiera och bedöma cyberhot på hela skalan kräver ofta omfattande samarbete mellan nationella myndigheter och med myndigheter i andra stater, inte minst genom etablerade samarbeten inom EU och Nato. Samarbete med näringsliv och ideella organisationer ger också viktiga bidrag. Organisationers olika informationsflöden kan innehålla viktig information både för den egna organisationen och för andra när det gäller cybersäkerhetsincidenter, sårbarheter och hot. Ett välfungerande samarbete med hög tillit aktörerna emellan lägger därför grunden för informationsdelning och varningar om relevanta hot och sårbarheter, men också för att utreda och attribuera angrepp.

Önskat läge 2030

NIS 2-direktivets och cyberresiliensförordningens krav om samordnad delgivning av information om sårbarheter bidrar till ökad informationsdelning om sårbarheter som upptäcks i produkter och tjänster. NCSC har väletablerade metoder för internationellt och privat-offentligt samarbete. Positiva exempel inom privat-offentlig samverkan har vidareutvecklats. Plattformar för att dela säkerhetsrelaterad information etableras, både inom och mellan offentlig och privat sektor, som möjliggör ökad delning och analys av realtidsinformation på teknisk och operativ nivå. Genom ökad analys av sådan information stimuleras även organisationers möjlighet att implementera, och dela med sig av förslag på, relevanta säkerhetshöjande åtgärder. Arbetet bidrar också till utvecklade och ändamålsenliga lägesbilder från NCSC till gagn för olika målgrupper samt vidareutvecklad samverkan mellan relevanta myndigheter om attribueringsfrågor. Informationsdelning sker, utifrån lagstiftning och etablerade processer, till gagn för alla inblandade parter och stärker bland annat förmågan att identifiera, hantera och utreda incidenter och angrepp.

Ett utökat internationellt samarbete på cyberområdet bidrar till värdefulla lärdomar om bland annat informationsdelningsmetoder som anpassas till svensk kontext. Privat-offentlig samverkan bidrar till ökad förmåga att upptäcka och motstå cyberangrepp vare sig de utgör en enskild händelse eller en del av en hybridaktivitet.

Industri.

Foto: Per Pixel Petersson/Image Bank Sweden

Mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter

En effektiv samordning är av central betydelse vid cybersäkerhetsincidenter. Lärdomar och erfarenheter behöver få genomslag i utvecklingen av nationell incidenthanteringsförmåga. Anmälnings- och rapporteringsbenägenheten vid incidenter behöver stimuleras, samtidigt som utmaningarna med överlappande rapporteringskrav behöver hanteras. För att effektivt nyttja de samlade utredande och förebyggande resurserna på cybersäkerhetsområdet behöver också myndigheters informationsdelning om incidenter vara ändamålsenlig. Sveriges förmåga att identifiera, hantera och bemöta cybersäkerhetsincidenter ska stärkas.

Önskat läge 2030

Statliga myndigheter utvecklar kontinuerligt den nationella operativa förmågan för stöd och hantering vid cybersäkerhetsincidenter. NCSC utvecklar och stärker Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. Privat-offentligt samarbete kring cybersäkerhetsincidenter har utvecklats och nyttjar den incidenthanteringskompetens som finns i privat sektor. Organisationer inom berörda sektorer har NCSC som kontaktpunkt vid hantering av cybersäkerhetsincidenter[1]. Regelbundna incidentövningar sker inom och mellan organisationer. Nationell övningsverksamhet fortsätter bedrivas och utvecklas. Statliga myndigheter har etablerat gemensamma plattformar för incidentrapportering vilket underlättar för organisationer både att utföra sin rapporteringsplikt och att få återkoppling och stöd samtidigt som ökad informationsdelning mellan relevanta myndigheter förenklas. Statliga myndigheters kommunikation om förmågehöjande åtgärder relaterat till sannolikhet eller konsekvens för en incident sker löpande. Kommunikation mellan mottagande statliga myndigheter och drabbade organisationer, under och efter att en cybersäkerhetsincident inträffat, utvecklas. Organisationers rapporterings- och anmälningsbenägenhet vid cybersäkerhetsincidenter ökar.

Sverige har också aktivt deltagit i samordnad hantering av storskaliga cybersäkerhetsincidenter inom ramen för samarbetsförfaranden på EU-nivå och bidragit till ett effektivt gränsöverskridande samarbete på operativ nivå mellan medlemsstaterna.

1 Detta gäller dock inte för exempelvis säkerhetshotande händelser enligt säkerhetsskyddsförordningen.

Mål 13: Utvecklad förmåga att förebygga och bekämpa cyberbrott

Cyberbrott utvecklas ständigt och genererar stora brottsvinster. Detta medför utmaningar för rättsvårdande myndigheter och ett behov av kontinuerligt utvecklingsarbete för att möta nya utmaningar. Den ökande andelen brott med digitala element belyser kopplingen mellan cybersäkerhetsarbetet och bekämpningen av cyberbrottslighet, där stärkt cybersäkerhet leder till färre cyberbrott. Detta understryker vikten av att brottsbekämpande myndigheter behöver öka sina förmågor att utreda och lagföra digitala brott.

Anmälningsbenägenheten till brottsbekämpande myndigheter behöver också öka. Mängden cyberangrepp mot svensk, digital kritisk infrastruktur eller enskilda personer från utlandet visar att det är viktigt att Sverige deltar aktivt i internationella samarbeten som syftar till att bekämpa ransomware-angrepp och datastölder.

Önskat läge 2030

Brottsbekämpande myndigheters utveckling av specialistfunktioner för cyberbrottslighet har inneburit en förbättrad förmåga att bekämpa denna brottslighet. Samarbetet mellan NCSC och brottsbekämpande myndigheters specialistfunktioner har bidragit till bättre lägesbilder. De brottsbekämpande myndigheternas förmåga att inhämta information i digitala system och från kommunikationstjänster har utvecklats. Därtill har lagstiftningen utvecklats, bland annat genom EU:s förordning om europeiska bevarande- och utlämnandeorder för elektroniska bevis. Bekämpningen av den kriminella ekonomin har förstärkts och brottsvinsterna från cyberbrott har minskat.

Statliga myndigheters kompetensförsörjning när det gäller digital brottsbekämpningsförmåga har stärkts och kunskapen om kriminella aktörers tillvägagångssätt och effekter av motåtgärder har ökat. De operativa samarbetsmöjligheter som erbjuds av Eurojust och Europol har förstärkts och nyttjas i större omfattning.

Berörda statliga myndigheters stöd och rådgivning om hantering och förebyggande av cyberbrottslighet har ökat. Brottsförebyggande samarbeten mellan ideell sektor, näringslivet och statliga myndigheter har vidareutvecklats. Mörkertalen för rapporterade digitala brott har minskat och närmar sig i vart fall rapporteringsgraden för fysiska brott.

En ökad förmåga att bekämpa cyberbrott har bidragit till en ökad trygghet för individer och organisationer i Sverige samt, givet att statliga hotaktörer kan använda kriminella grupper som mellanhänder för olika former av hybridaktiviteter, till att Sveriges samlade förmåga att motstå hybridhot har förstärkts.

Telekommunikation

Foto: MSB

Genomförande och uppföljning

Den nationella strategin för cybersäkerhet ger inriktningen för regeringens arbete med frågor av betydelse för Sveriges cybersäkerhet. Strategin kommer regelbundet och minst vart femte år att utvärderas på grundval av strategins resultatindikatorer i enlighet med NIS 2-direktivets krav.

Av bilagd handlingsplan framgår att strategin kommer att omsättas i konkret handling bland annat genom specifika uppdrag och styrning av myndigheter. Det kan också krävas andra regeringsbeslut för att genomföra strategin i denna del. Teknik- och hotutvecklingen innebär att cybersäkerhetsområdet förändras och utvecklas i snabb takt och det krävs därför flexibilitet i genomförandet av strategin. Handlingsplanens innehåll kommer därför att uppdateras löpande. Därutöver kommer utvärdering och revidering av handlingsplanens innehåll att ske på det sätt som regeringen ser behov av. Bilagan som gäller organisationer med roller och ansvarsområden inom cybersäkerhet kommer också att behöva uppdateras, bland annat när den nationella regleringen som genomför NIS 2-direktivet i Sverige har trätt i kraft. Denna uppdatering kommer att ske på det sätt och i den form som regeringen ser behov av.

Begreppsförteckning

Allriskperspektiv: Används i denna strategi på motsvarande sätt som allriskansats i skäl 79 i NIS 2-direktivet.

Cyberresiliensförordningen: Förordningen innebär bland annat att vissa kritiska produkter och tjänster omfattas av högre säkerhetskrav (bland annat bedömning av överensstämmelse samt tredjepartsgranskning enligt EU:s New Legal Framework och CSA:s ramverk för cybersäkerhetscertifiering).

Cybersäkerhetsakten: Akten reglerar bland annat cybersäkerhetscertifiering på den inre marknaden som möjliggör att olika it-produkter och it-tjänster (till exempel molntjänster) kan certifieras mot en ensad, kvalitetssäkrad och gemensam uppsättning krav. Sådan certifiering kan bland annat användas vid myndigheters kravställning i samband med upphandling, som krav i tillsyns- och sektorsmyndigheters föreskrifter eller för att visa uppfyllnad av olika cybersäkerhetskrav vid myndighetstillsyn.

Cyber range: Testbädd och övningsanläggning för cybersäkerhet.

Cyberangrepp: En interaktion mellan en angripare och ett mål som i) angriparen inte har rätt att utföra mot målet, ii) medför ett utbyte av information som resulterar i en interaktion, konfigurering, installation/sparande, avinstallation/raderande eller överbelastning i något av målets informationssystem, iii) resulterar i minst en för målet oönskad konsekvens i termer av konfidentialitet, riktighet eller tillgänglighet för målet eller för andra via målet och vi) som angriparen utför i ett antagonistiskt syfte.

Cybersäkerhet: Används i denna strategi i enlighet med NIS 2-direktivet, som nyttjar cybersäkerhetsaktens definition (all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot).

Digital leveranskedja: Tjänster och infrastruktur som levererar eller möjliggör leverans av digitala produkter vilka används för att upprätta, upprätthålla, utveckla eller återställa en verksamhets informationshantering och informationssystem.

IoT: Internet of Things, eller Sakernas internet, rör användandet av uppkopplade föremål i verksamheter.

Helikopter över svenskt skogslandsskap.

Foto: Hampus Hagstedt/Försvarsmakten

Konfidentialitet: En aspekt av cybersäkerhet som innebär att endast behöriga kan ta del av informationen. Frågor som rör offentlighetsprincipen och allmänhetens tillgång till handlingar faller dock utanför denna definition.

Monoberoende: Tjänster eller infrastruktur som organisationer är beroende av och där alternativ saknas om den aktuella tjänsten eller infrastrukturen skulle upphöra.

NIS2-direktivet: 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).

Nätverks- och informationssystem: Ett nätverks- och informationssystem enligt definitionen i artikel 4.1 i direktiv (EU) 2016/1148.

Ransomware: Utpressningsvirus och program som krypterar hela eller delar av en verksamhetsinformation som lagras på drabbade informationssystem och gör informationen otillgänglig. Syftar till att försöka utpressa en organisation eller individ på en lösensumma. Angrepp kan även genomföras i syfte att nå specifik information, till exempel för underrättelseinhämtning.

Riktighet: En aspekt av cybersäkerhet som innebär att information och informationssystem är korrekta eller fungerar korrekt och inte ändras på ett felaktigt sätt.

Systematisk cybersäkerhet: Förebyggande och kontinuerlig anpassning av skydd utifrån behov och risker. Det innefattar arbetssätt baserat på en metodik för verksamhetsrisk, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet, det vill säga skydd av informationstillgångar som gäller konfidentialitet, riktighet och tillgänglighet.

Tillgänglighet: Tillgänglighet är aspekten att information eller informationssystem ska finnas tillgängligt när de behövs.

Överbelastningsangrepp: Angreppsmetod som bygger på att stora mängder datatrafik eller förfrågningar skickas mot en server eller annan nätverkskomponent i syfte att begränsa dess förmåga att bearbeta data och därmed blockera åtkomst för annan, legitim datatrafik.

Regeringskansliet
Växel: 08-405 10 00
www.regeringen.se