Policy för cybersäker upphandling

Nulägesbeskrivning och analys sammanställdes i oktober 2025. Dessa kommer att uppdateras till slutversionen av policyn.

Nulägesbild

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 fingervisnig. I en rapport från Tech Sverige[1] uppges att techbranschens omsättning 2022 var över 1000 miljarder kronor och att dess bidrag till Sveriges BNP uppgick till ca 350 miljarder kronor eller 7.9% av BNP .

Det finns ingen 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% av BNP[2]. Inom EU finns över 250 000 upphandlande offentliga entiteter och ca. 14% av EU:s BNP läggs på offentlig upphandling, något som motsvarar ca 2 biljoner euro per år[3]. Alla länder inom EU har motsvarigheter till den svenska svenska regleringen om offenlig upphandling då regelverken bygger på samma EU-direktiv.[4] Regleringen är till för att gynna den inre marknaden och främja konkurrens, transparens, effektivtet och innovation inom hela unionen. Företag i ett medlemsland ska ha goda möjligheter till att göra affärer med offentliga aktörer i de andra.

I Sverige regleras offentliga upphandlingar främst genom lagen om offentlig upphandling, LOU.[5] Syftet med regleringen är att säkerställa att offentliga medel i Sverige används effektivt, transparent och att konkurrensen gynnas. Statliga myndigheter, regioner,

[1] https://techsverige.se/app/uploads/2023/11/TECH-SVERIGE-RAPPORT-SVENSKA-TECHBRANSCHEN-2023.pdf
[2] https://www.upphandlingsmyndigheten.se/nyheter/2025/upphandling-for-1-009-miljarder/
[3] https://single-market-economy.ec.europa.eu/single-market/public-procurement_en
[4] Europaparlamentets och rådets direktiv 2014/24/EU
[5] LOU, SFS 2016:1145

kommuner och offentligt ägda bolag är alla skyldiga att följa LOU vid inköp av varor, tjänster och för byggentreprenad där kostnaderna beräknas överstiger vissa tröskelvärden. Det finns även särskild lagstiftning utöver LOU för olika sektorer, exempelvis lagen om upphandling på försvars- och säkerhetsområdet (LUFS)[6], lagen om upphandling inom vatten, energi, transporter och posttjänster (LUF)[7] samt lagen om upphandling av koncessioner (LUK)[8]. LUFS reglerar upphandlingar som har betydelse för rikets säkerhet, så som försvarsmateriel och säkerhetstjänster.

Cybersäkerhetsläget gällande upphandling i Sverige

Det finns ingen samlad statistik över hur många offentliga upphandlingar som ställer specifika krav på cybersäkerhet eller hur sådana kravs följs upp. Därmed saknas också analyser av vilka eventuella effekter cybersäkerhetskrav får på till exempel säkerheten i produkter och tjänster eller på företagens möjligheter att leverera produkter och tjänster. Det är också oklart om det finns skillnader mellan organisationer i olika sektorer gällande om krav ställs på säkerheten ställs och i så fall vilka krav som ställs.

Mätningar av cybersäkerheten i Sverige har genomförs vid fyra tillfällen mellan år 2021-2025 genom Myndigheten för samhällsskydd och beredskap, MSB:s verktyg, Cybersäkerhetskollen[9]. Verktyget riktar sig i första hand till aktörer inom offentlig förvaltning och företag som omfattas av NIS-regleringen men alla organisationer uppmuntras att delta. Utifrån inrapporterade resultat[10] 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% av kommunerna att de saknat arbetssätt för att säkerställa informationssäkerhet vid upphandling under de senaste två åren, ca. 75% av regionerna hade inte följt upp om krav som ställts vid upphandlingar varit tillräckliga eller om leverantörer uppfyllt ställda krav. En stor majoritet av myndighterna hade inte följt upp eller utvärderat arbtessätten vid upphandling för att säkerställa att de omhändertagit informations- och cybersäkerhet i tillräcklig omfattning.

Narionellt Cybersäkerhetscentrum (NCSC) lyfter i rapporten ”Cybersäkerhet i Sverige 2024” att otillräcklig kravställning gällande cybersäkerhet är ett problem för cybersäkerheten, samhället i stort och att det krävs relevant kompetens inom cybersäkerhetbåde vid anskaffning av varor och tjänster samt vid utkonraktering av it-infrastruktur. NCSC nämner i rapporten att tydliga avtal och krav som utgår från standarder som viktiga områden att arbeta med för att möta problemen. Man lyfter också risker förnkippade med att många underleverantörer inte bedriver tillräckligt

[6] https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-20161145-om-offentlig-upphandling_sfs-2016-1145/
[7] https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-20161146-om-upphandling-inom_sfs-2016-1146/
[8] https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-20161147-om-upphandling-av-koncessioner_sfs-2016-1147/
[9] https://www.msb.se/sv/publikationer/resultatredovisning-av-cybersakerhetskollen-2024--det-systematiska-cybersakerhetsarbetet-i-den-offentliga-forvaltningen/
[10] https://rib.msb.se/filer/pdf/30971.pdf

cybersäkerhetsarbete. Tendiums senaste rapport (2024)[11] visar en ökning i förekomsten av ordet "cybersäkerhet" i underlag för it-upphandlingar de senaste åren.

Stöd och vägledning vid upphandling

För att underlätta och utveckla offentlig upphandling erbjuds stöd och vägledning till både köpande och levererande sida. Upphandlingsmyndigheten erbjuder vägledningar, mallar och kriteriebibliotek för kriterier omhållbarhet - främst miljö och social hållbarhet. liksom en frågetjänst där det är öppet för alla att ställa frågor om offentlig upphandling. Även aktörer som Konkurrensverket och Kammarkollegiet publicerar olika typer av stöd med visst fokus på köpande sida. SKR:s inköpscentral Adda tillhandahåller stöd för SKR:s medlemmar i upphandlingsfrågor. Även intresseorganisationerna Företagarna och Svenskt Näringsliv samt myndigheterna Tillväxtverket och Upphandlingsmyndigheten erbjuder stöd direkt riktat till leverantörer. För den som ska genomföra en upphandling av IKT-produkter och IKT-tjänster finns både generellt och specifikt stöd. Specifika stöd riktar sig till en viss målgrupp, typ av organisationer, eller avser en vissa produkt eller tjänst. Följande är exempel på sådana stöd:

- Förslag på kravtexter till upphandlingar av it-system och digitala tjänster från Digg.[12]
- Rekommendationer för upphandling av data från Digg.[13]
- Informationssäkerhet vid upphandling från Upphandlingsmyndigheten.[14]
- Security Guide for ICT Procurement från ENISA[15]
- Good Practices for Supply Chain Cybersecurity från ENISA[16]
- KLASSA, ett verktyg som hjälper organisationer att välja säkerhetskrav från SKR.[17]
- Kunskapsstöd för e-hälsa från E-hälsomyndigheten, som 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.[18]

---

11 https://upphandling24.se/wp-content/uploads/2025/05/Rapport-Offentlig-upphandling-2024-Tendium.pdf
12 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
13 https://www.digg.se/kunskap-och-stod/oppna-och-delade-data/offentliga-aktorer/rekommendationer-for-upphandling-av-data
14 https://www.upphandlingsmyndigheten.se/regler-och-lagstiftning/andra-regler-som-kan-bli-aktuella/informationssakerhet-vid-upphandling/
15 https://www.enisa.europa.eu/publications/security-guide-for-ict-procurement
16https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practices%20for%20Supply%20Chain%20Cybersecurity.pdf
17 https://klassa.skr.se/
18 https://www.ehalsomyndigheten.se/yrkesverksam/e-halsostod-till-kommuner/kunskapsstod-for-e-halsa/sok-bland-kunskapsstoden-for-e-halsa/

- Säkerhetspolisens vägledning om skyldigheter vid exponering av säkerhetsskyddad verksamhet[19]
- Säkerhetspolisens vägledningar om säkerhetsskydd.[20]

MSB 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 ställa säkerhetskrav vid en upphandling som uppfyller det behov av skydd som informationen 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.[21]
- Metodstöd för systematiskt informationssäkerhetsarbete somger stöd vid genomförade av informationssäkerhetsarbete i en organisation och vilka krav som bör ställas på en leverantörs informationssäkerhetsarbete.[22]
- Vägledningen säkerhet i informationssystem som stödjer med krav som kan behöva ställas på en leverantörs it-system it-miljö.[23]
- Publikationerna Grundläggande säkerhet i cyberfysiska system[24] och Ökad säkerhet i industriella informations- och styrsystem vilken ger stöd i att förstå de särskild krav som bör ställas vid upphandling av IKT-produkter och IKT-tjänster som kommunicerar med cyberfysiska system[25]
- Vägledningen för fysisk informationssäkerhet i it-utrymmen[26] är framtagen av MSB tillsammans med riksarkivet och beskriver hur man kan identifiera vilka krav på fysiskt skydd som kan behöva ställas på olika utrymmen där system finns (it-utrymmen).

Nationella krav på cybersäkerhet

Det finns flera lagar och förordningar med tillhörande föreskrifter som ställer krav på att skydda den information som en organisation skapar, behandlar, distribuerar eller lagrar. Regleringen omfattar antingen skyddet av informationsbehandlingen generellt eller fokuserar på en viss typ av information så som personuppgifter. Kraven i de olika regleringarna kan vara generella, exempelvis att informationsbehandlingen ska skyddas tillräckligt eller så ställer regleringen specifika krav på olika säkerhetsåtgärder. Av regeringens arbete med att införa NIS2-direktivet i Sverige framgår i propositionen att cybersäkerhetslagen ställer krav på organisatoriska, tekniska och driftrelaterade

[19]https://www.sakerhetspolisen.se/download/18.3222e1b7187a064b070e6/1683815514604/Skyldighet%20vid%20exponering%20av%20sa%CC%88kerhetska%CC%88nslig%20verksamhet_anpassad.pdf
[20] https://sakerhetspolisen.se/sakerhetsskydd/vagledningar-sakerhetsskydd.html
[21] https://rib.msb.se/filer/pdf/28742.pdf
[22] https://metodstod-informationssakerhet.msb.se/
[23] https://www.msb.se/sv/publikationer/vagledning--sakerhetsatgarder-i-informationssystem/
[24] https://www.msb.se/sv/publikationer/grundlaggande-sakerhet-i-cyberfysiska-system--vagledning/
[25] https://www.msb.se/sv/publikationer/vagledning-till-okad-sakerhet-i-industriella-informations--och-styrsystem/
[26] https://www.msb.se/sv/publikationer/vagledning-for-fysisk-informationssakerhet-i-it-utrymmen/

säkerhetsåtgärder samt de säkerhetsåtgärder som behövs för att skydda den fysiska miljön där system som behandlar informationen finns. Föreskrifter[27] förtydligar kraven skydda berörda organisationers informationsbehandling i nätverk och informationssystem genom att krav ställs på minst på säkerhetsåtgärderna

- riskanalys, incident-, kontinuitets- och krishantering, uppnå säkerhet i leveranskedjor, personalsäkerhet och utbildning i cybersäkerhet inklusive cyberhygien,
- kravställning och införande av lämpliga och proportionella säkerhetsåtgärder vid förvärv, utveckling och underhåll av nätverk- och informationssystem för att dessa ska uppnå tillräcklig säkerhet och hur effektiviteten i säkerhetsåtgärderna bedöms samt att tillgångarna förvaltas.
- åtkomstkontroll, autentisering, säker kommunikation, kryptografi, och nödkommunikationssystem.

Cybersäkerhetscertifiering, produktdeklarationer och andra krav

Cybersäkerhetscertifieringar

Det finns EU-gemensamma standarder för cybersäkerhetscertifiering för IKT-produkter och -tjänster skapas genom genom EU:s ramverk för cybersäkerhetscertifiering, i enlighet med Cybersäkerhetsförordningen. I Sverige har Försvarets materielverk, FMV, rollen som nationell myndighet för cybercertifiering. Certifikat som utfärdats för en IKT-produkt, IKT-tjänst eller IKT-process av ett europeiskt lands myndighet för cybersäkerhetscertifiering enligt regleringen är giltigt i hela unionen. Certifieringar kan börja utfärdas från 2025 genom den första certifieringsordnignen EUCC, vilken trädde i kraft 2024. Det första företaget certifierades tidigt 2025.

För att uppnå cybersäkerhetsmålen så rekommenderas i skälen till Cyberresiliensförordningen[28] att tillverkare upprättar en programvarudeklaration över de komponenter som ingår i en produkt med digitala element för att det ska bli enklare att göra en sårbarhetsanalys för produkten. En administrativ samarbetsgrupp (Adco) ska göra beroendebedömningar för EU:s marknad, särskilt för de komponenter som kan innehålla öppen eller fri programvara.

Krav på kryptering

Kryptering är en viktig säkerhetsåtgärd för att skydda information i digitala miljöer. Vid användning av kryptering bör enbart 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. Det saknas statistik över hur ofta det ställs särskilda krav på kryptering vid offentig upphandling i Sverige. För att hantera hotet från

[27] https://www.regeringen.se/regeringsuppdrag/2025/09/uppdrag-till-myndigheten-for-samhallsskydd-och-beredskap-att-forbereda-genomforandet-av-nis-2-direktivet/
[28] Cyberresiliensförordningen (EU 2024/2847)

kvantdatorer mot säkerhet i krypteringslösningar har EU tagit fram en färdplan i två delar för övergång till kvantsäkrad kryptografi inom unionen. Den första delen innehåller konkreta råd om aktiviteter som behöver vidtas av organisationer. Den andra delen kommer att innehålla bland annat mer detaljerade och utförliga rekommendationer rörande algoritmer.

Cybersäkerhetsprodukter med öppen källkod

Digg har publicerat Policy för anskaffning samt utveckling av programvara[29]där offentliga aktörer uppmanas att ha programvara med öppen källkod som huvudval vid upphandlingar. Policyn detaljeras i Riktlinjer för utveckling och publicering av öppen programvara[30]men det är ont om stöd för att närmare förstå vad en organisation behöver beakta vid utveckling av pgrogramvara eller val av produkter med öppen källkod. Det finns heller ingen statsitisk som visar på hur ofta krav på produkter och tjänster med öppen källkod ställs i offentliga upphandlingar, vilka krav som ställs eller hur utfallen då blir. Om det är skillnad mellan IKT-produkter generellt och för cybersäkerhetsprodukter specifikt gällande upphandling är också oklart.

I skälen till Cyberresiliensförordningen[31] anges att hård- och programvara som tillgängliggörs för den europeiska marknaden ska utvecklas så att säkerhet omhändertas i produktens hela livscykel för att minska antalet sårbarheter i IKT-produkter. I artikel 13 ställs krav på stor riskmedvetenhet vid integrering av programvara med fri och öppen källkod i produkter. Det ska finnas dokumentation om hur programvara med öppen källkod har utvecklats för att omhänderta ställda säkerhetskrav för att användare ska kunna bedöma säkerheten i ingående programvaror vid val av IKT-produkter.

Relaterade svenska initiativ för att öka cybersäkerheten

Regeringen beslutade 2024 om förordningen om samordnad och säker statlig it-drift[32] för att öka säkerheten och kostnadseffektiviteten hos statliga myndigheter genom tillgång till moderna, säkra och kostnadseffektiva it-verktyg och it-tjänster. Syftet är att säkerställa en säker, effektiv och samordnad statlig it-drift som möjliggör för statliga myndigheter att bedriva sina verksamheter genom hela hotskalan.

I betänkandet från interoperabilitetsutredningen[33] lyfts att nuvarande arbetssätt där organisationer i den offentliga förvaltningen skyddar sin information utifrån vad organisationen vet och det är utifrån den egna organisatoriska förutsättningar och behov. Det försvårar datautbyte och medför att. samhällets övergripande behov av information och skydd för informationen blir svårt att omhänderta. Utredningen föreslår därför att det

[29] Policy för anskaffning samt utveckling av programvara (Digg, 2022)
[30] Riktlinjer för utveckling och publicering av öppen programvara (Digg, 2022)
[31] Cyberresiliensförordningen (EU 2024/2847)
[32] https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-20241005-om-samordnad-och-saker_sfs-2024-1005/
[33] https://www.regeringen.se/contentassets/6866c386b0ec492c8171c92c9c8922cf/en-reform-for-datadelning-sou-202396.pdf

tas fram koordinerade skyddsnivåer som ett sätt underlätta för offenlig sektor att ställa säkerhetskrav och visa hur säkerhetskrav är uppfyllda vid datadelning.

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

Inom ramen för NCSC[34] 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.

Analys av nuläge

Det är positivt att det idag finns många initiativ för att underlätta för offentliga aktörer att ställa cybersäkerhetsrelatede krav i upphandlingar av IKT-produkter och IKT-tjänster. Det finns ett antal förslag till och påbörjade initiativ med att samordna cybersäkerhetskrav för att underlätta kravställningen för offenlig 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 statisitk från Cybersäkerhetskollen att upphandling är ett område där utvecklingen kring stärkt cybersäkerhet inte går i den takt som behövs. Några av de centrala utmaningsområdena är:

- Många verksamheter som genomför it-upphandlingar saknar tillräckilga resurser och adekvat cybersäkerhetskompetens. En av de bakomliggande orsakerna är den snabba digitaliseringen som skapat ökade behov av personal med sådan kompetens i en högre takt än vad som finns tillgängligt. Konsekvenserna av bristande resurser och kompetens blir IT-upphandlingar som inte ställer lämpliga, tillräckliga eller träffsäkra krav vilket i sin tur kan leda till bland annat osäkra lösningar eller att krav ställs på onödigt hög säkerhet med höga avgifter till följd.
- Förmågan att följa upp följa upp avtal, effektmål och krav saknas hos många upphandlande organisationer. De bakomliggande orsakerna handlar om begränsade resurser och bristfällig strategisk förmåga eller kompetens att omhänderta offentlig upphandling och avtalsuppföljning. Konsekvensen blir osäkerhet kring att leveranserna möter de krav som ställts eller en tillit till att leverantören förstått och uppfyller de krav som ställts.
- 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 också 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,

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

målgrupp och förmåga att upprätthålla kvalitén i stödmaterialet samt bristfällig 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 maximal effekt. Det kan också innebära att föråldrat eller felaktigt stöd används vilket leder till att organisationen inte ställer rätt krav utifrån sina behov.

- Att ta fram gemensamma säkerhetskrav och strukturera dem i skyddsnivåer kommer inte fullt ut ersätta det arbete varje organisation måste göra utifrån den informationsbehandling de ska göra och riskerna som är förknippade med den. Även om ett stöd i form av rekommenderade säkerhetsåtgärder kan underlätta för båda beställare och leverantörer om vilka säkerhetskrav en produkt eller tjänster behöver uppfylla kan sådana krav leda till att organisationens behov av säkerhet inte uppfylls. Konsekvensen blir att organisationen köper produkter eller tjänster som inte möter deras behov eller får en produkt eller tjänst med mer säkerhet än den specifika informationsbehandlingen behöver.

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240 Fax: 010-240 56 00
registrator@msb.se www.msb.se
Org.nr: 202100-5984