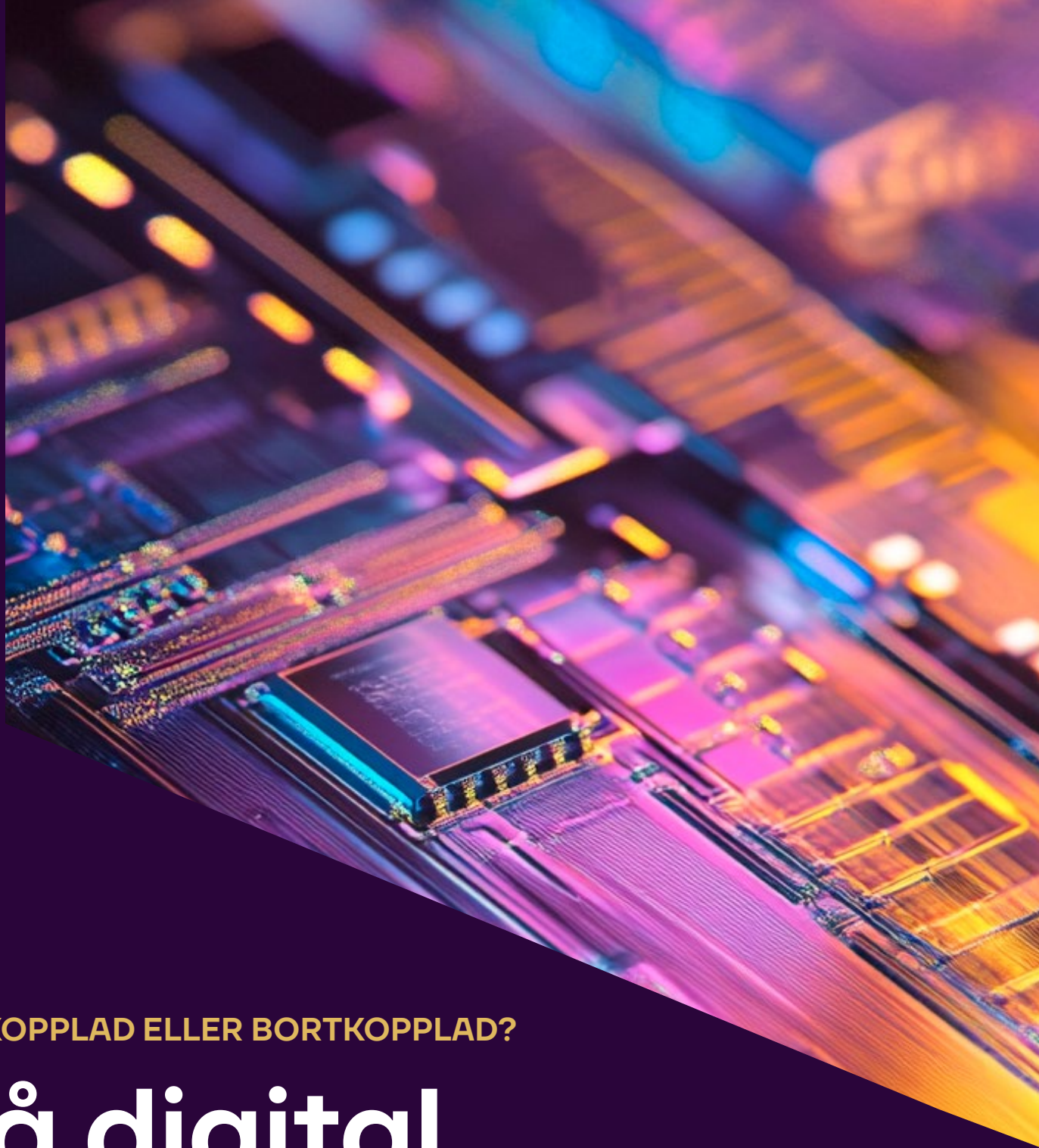
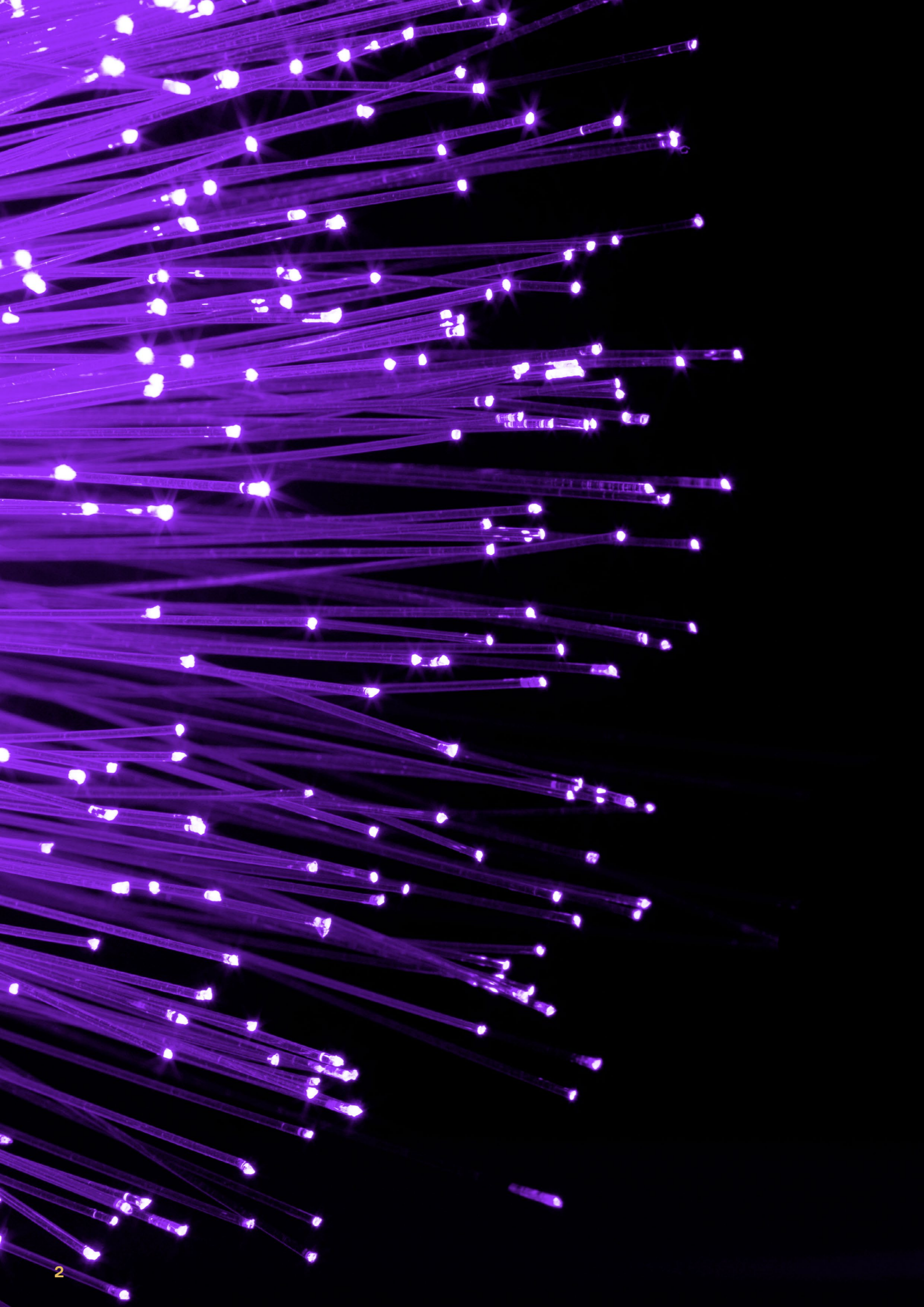




UPPKOPPLAD ELLER BORTKOPPLAD?

Så digital är svensk teknikindustri 2025



UPPKOPPLAD ELLER BORTKOPPLAD?

Innehåll

- 4 Om rapporten
- 5 Sammanfattning
- 7 Innebörden i teknikindustrins digitalisering
 - 7 Den digitala transformationen
 - 8 Digital mognadsgrad inom teknikindustrin
 - 9 Digitaliseringens påverkan på teknikindustrin
 - 10 Användningen av digital teknik inom teknikindustrin
 - 11 Användning av AI inom teknikindustrin
 - 12 Hur används AI idag
 - exempel från Teknikföretagens medlemsföretag
 - 13 Kunskapen kring AI inom teknikindustrin
 - 14 Hinder för AI tillämpningar
 - 14 Strategiska områden för teknikindustrin
 - 15 Industriellt tillämpad AI
 - 16 Cyberhotet mot teknikindustrin
 - 16 Cybersäkerhet inom teknikindustrin
 - 17 Cyberattacker mot teknikindustrin
 - 18 Krav på cybersäkerhet inom teknikindustrin
 - 19 Lagstiftning om cybersäkerhet
- 20 Rekommendationer för att stärka teknikindustrins digitalisering
- 22 Bilaga

Om rapporten

Denna rapport innehåller en sammanställning av hur digitaliseringsarbetet inom teknikindustrin i Sverige fortlöper. Resultaten baseras på ett urval av cirka 500 medlemsföretag hos Teknikföretagen som svarat på en webbaserad enkät. Företagen är relativt representativa för Teknikföretagens medlemmar med avseende på företagsstorlek och geografisk lokalisering. Även om utvecklingen kan skilja sig mellan enskilda företag ger de redovisade resultaten sammantaget en tämligen tillförlitlig bild över status och hur digitaliseringen fortskrider.

Teknikföretagen är en bransch- och arbetsgivarorganisation med 4 500 medlemsföretag. Tillsammans står dessa företag för hälften av näringslivets investeringar i FoU, en tredjedel av Sveriges export och sysselsätter över en miljon människor. Medlemsbasen sträcker sig från globala industrijättar som Ericsson, Scania, AFRY, ABB och Volvo till små och medelstora företag i alla storleksklasser. En gemensam nämnare för samtliga medlemmar är att digitaliseringen är ett verktyg som omformar deras verksamhet. För att behålla sin konkurrenskraft måste de både utnyttja teknikens möjligheter och hantera dess utmaningar.

Stockholm, april 2025

Sammanfattning

Hur går det med digitaliseringen?

Den digitala transformationen har över tid ökat i hastighet, med stora investeringar och snabb utveckling av ny digital teknik.¹ För teknikindustrin innebär det ett behov av kontinuerligt arbete för att omforma och utveckla verksamheten. Så har också skett. Den digitala mognadsgraden är i nuläget (2025) relativt hög bland teknikföretag med verksamhet i Sverige och fortsätter att utvecklas. Företagen har med andra ord relativt god förståelse av den digitala tekniken, hur den kan tillämpas och använder den också på ett ändamålsenligt sätt. Digitaliseringen påverkar hela teknikindustrins verksamhet – från produktdesign till eftermarknad – men just nu berör den, i särskilt hög utsträckning, administration och produktion.

Hur används digital teknik så som AI?

Företagen i teknikindustrin använder simultant flera olika typer av digitala tekniker i sin verksamhet. Sensorer, robotar och system för dataanalys knyts ihop med molntjänster och understryker behovet av snabb, tillförlitlig uppkoppling (konnektivitet). Stora företag (fler än 250 anställda) har generellt sett många olika tillämpningar och därmed också behov av flera olika digitala tekniker, inklusive AI. AI-användningen är påtagligt större bland företag med många anställda, men oavsett företagsstorlek framhålls att svårighet att få tillgång till kompetens inom AI och den reella möjligheten att prioritera denna teknik håller tillbaka en snabbare implementering.

Hur står det till med cybersäkerheten?

Totalt sett har de digitala attackerna mot aktörer i Sverige ökat², men bland Teknikföretagens medlemmar förefaller det som att andelen som identifierat att de blivit angripna har minskat. Grundläggande tekniska funktioner (som virusskydd och brandväggar), regler för användning och främjande av en säkerhetskultur har sannolikt bidragit till att öka medvetenheten om attacker och skapat en högre skyddsnivå. Samtidigt har attackerna blivit mer sofistikerade och svåra att upptäcka. Därtill finns utmaningar med kravställning och påtaglig okunskap runt de lagkrav för cybersäkerhet som nu införs, exempelvis NIS2.

¹ SCB, "Företagens utgifter för IT", <https://www.scb.se/>

² De registrerade cyberattackerna under kvartal fyra 2024 ökade globalt med 75 procent jämfört med samma kvartal 2023. Ökningen var särskilt påtaglig i Sverige. Här ökade de identifierade attackerna med 165 procent jämfört med samma period. Akademi, myndigheter, sjukvård och aktörer kopplade till militär verksamhet var mest utsatta. Check Point Research, "Cyberattacker ökar med 165 procent i Sverige – största ökningen i Europa", <https://www.voister.se/artikel/2024/10/cyberattacker-mot-sverige-okar-mest-i-europa/>

Vad behöver göras?

Digitalisering kommer i många former och inkluderar överlappande tekniker och kompetenser samt, i ökad utsträckning, lagkrav. Digital transformation är därmed en ledningsfråga som behöver hanteras strategiskt, av varje enskilt företag, utifrån den enskilda verksamhetens förutsättningar.

Generellt behöver företagen:

- Kunna erbjudas stöd och konsultation i uttolkning av de lagkrav som ställs upp av myndigheterna i Sverige och på europeisk nivå. Det är väsentligt att myndigheter så som länsstyrelsen kan ge vägledning och är beredda att kunna besvara frågor kring hur lagar ska tolkas och omsättas.
- Ges möjlighet att delta i ett digitaliseringslyft för att öka baskunskapen hur digital teknik kan användas och integreras samt hålla jämna steg med utvecklingen inom bland annat konnektivitet, AI och cybersäkerhet.
- Få ökad tillgång till relevant kompetens, inte minst personer som har verksamhetsnära kunskap inom AI. Här spelar lärosätena i allmänhet och RISE i synnerhet en central roll för att säkerställa att forskning och utveckling kan nyttiggöras.

Ur ett nationellt perspektiv är det därtill viktigt att digital teknik ges prioritet. Inom forsknings- och innovationspolitiken behöver exempelvis strategiska områden för industrin så som elektronik, konnektivitet och mjukvaruutveckling tilldelas resurser. Riktade insatser i form av innovationsprogram som *Avancerad Digitalisering*, *Net Zero Industry* och *Smartare elektronikersystem* utgör verktyg för att samla kompetenser och utveckla innovativa lösningar på gemensamma industriella utmaningar där digital teknik utgör kärnan. Det krävs också goda möjligheter att testa och utvärdera digitala lösningar, särskilt för att säkerställa en adekvat skyddsnivå – med andra ord funktioner för att förhindra, hantera och minimera konsekvenserna av digitala attacker.



Innebörden i teknikindustrins digitalisering

Den digitala transformationen

Digitalisering hos Teknikföretagens medlemmar avser primärt användning av digital teknik för att koppla upp och koppla samman produkter, system och processer. Det inkluderar också extrahering och analys av data. Utmärkande drag för de digitala teknikerna är bland annat att de förstärker varandra, att de utvecklas snabbt och att de är föränderliga. Nya funktioner och användningssätt tillkommer ständigt. För att hålla jämna steg med utvecklingen och ha förmåga att dra nytta av den digitala tekniken krävs att företagen gör betydande investeringar, vilket även inkluderar kontinuerlig kompetensuppbyggnad.

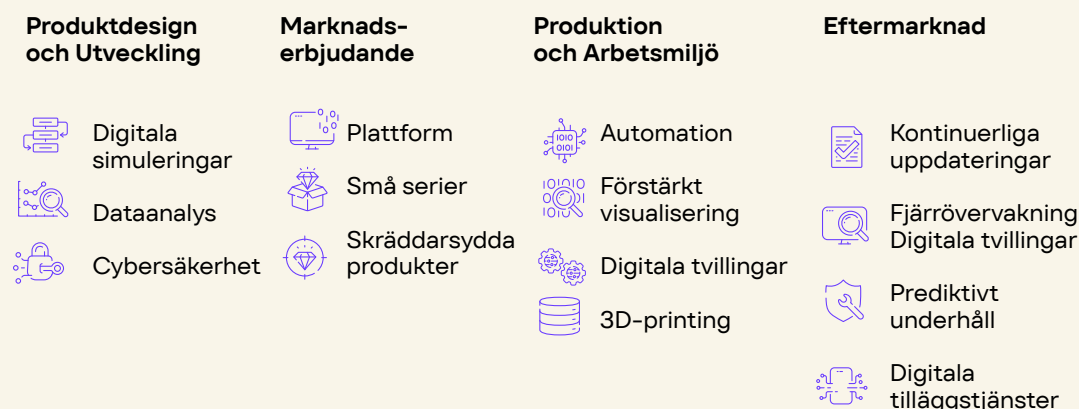
För teknikindustrin håller den digitala tekniken gradvis på att förändra affärs- och produktionsförutsättningar på flera sätt. Simuleringar och analys av stora datamängder skapar exempelvis nya möjligheter för hur produkter kan designas. Det blir dessutom möjligt att bygga in mekanismer som ger förstärkt säkerhet. Den digitala tekniken gör det också lättare att skapa interoperabilitet och gemensamma plattformar, tillika att skräddarsy produkter efter önskemål samt tillhandahålla produkter i mycket små serier till rimlig kostnad.

Förändringen som digital teknik medger syns även i produktionen. Exempelen är många och sträcker sig från ökad automation genom exempelvis avancerade industrirobotar till effektivare sammansättning genom förstärkt visualisering. Digitaliseringen möjliggör också en säkrare arbetsmiljö genom statusövervakning via digitala tvillingar samt möjlighet att använda 3D-printing för nya komponenter och material, vilket leder till minskad resursförbrukning och klimatavtryck.

Den digitala tekniken ger också möjlighet till en förstärkt eftermarknad där det finns stort potentiellt värdeskapande i att erbjuda nya funktioner, uppdateringar och prediktivt underhåll. Detta bidrar gradvis till en tjänstefiering som kan realisera stora värden, i form av nya affärsmöjligheter. (Se figur).

Figur 1. Hur påverkar digitaliseringen teknikindustrin?

- Uppskattade väsentliga förändringar genom digital teknik på affärs- och produktionsförutsättningar hos Teknikföretagens medlemmar, 2025



Digital mognadsgrad inom teknikindustrin

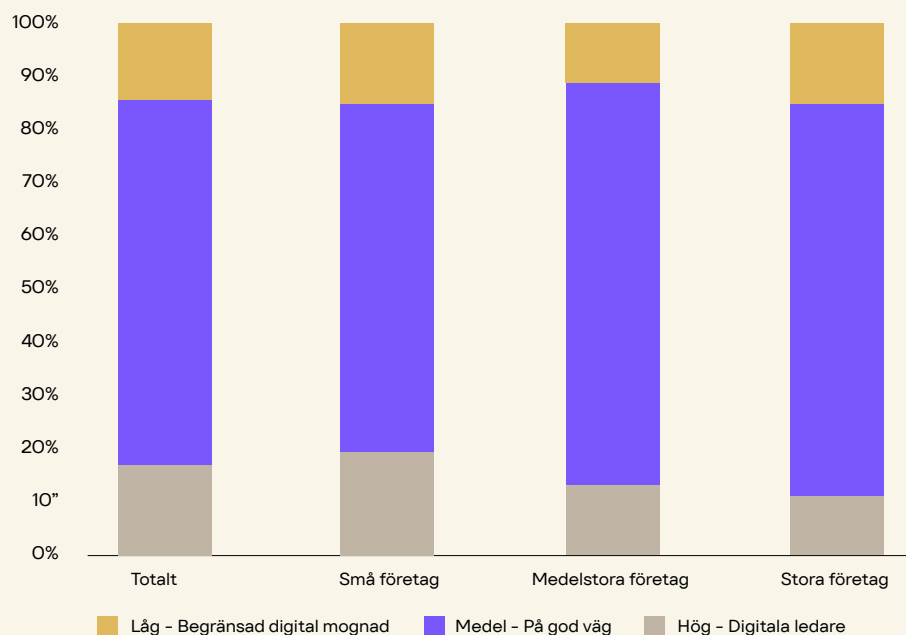
Som redogörs för ovan är möjligheterna med den digitala tekniken stor och består av flera olika komponenter som påverkar hela företagets verksamhet, inte minst hur det leds och organiseras. En konsekvens av detta är att det är en utmaning att exakt avgöra den digitala mognadsgraden, det vill säga om det finns en god förståelse av digital teknik, hur den kan tillämpas och om den används på ett ändamålsenligt sätt.

Vid en självskattning av den digitala mognadsgraden uppger majoriteten av de tillfrågade medlemsföretagen hos Teknikföretagen, knappt 70 procent, att de har passerat de första stegen och nu har ett systematiskt digitaliseringsarbete. De upplever med andra ord att de är på rimligt god väg med grundläggande användning och nyttiggörande av digitala teknik i sin verksamhet. Därtill finns ungefär 15 procent som i det närmaste kan klassas som digitala ledare. Dessa företag bedömer själva att deras digitala mognadsnivå är hög, vilket bland annat kan innefatta att de integrerat digitala verktyg och satsat på att dra full nytta av digitaliseringens möjligheter genom att förändra sina affärsmodeller, processer och produkter.

På motsatt sida om pionjärerna står strax över 15 procent av Teknikföretagens medlemmar som fortsatt gör bedömningen att deras digitaliseringsarbete släpar efter och att de i förhållande till industrin som helhet har en låg grad av digitalisering. De har med andra ord en längre startsträcka och upplever att utvecklingen går så fort att de har svårt att hålla jämna steg med konkurrenter och partners.

Det kan noteras att alla de tre digitala mognadsgraderna återfinns hos alla företagsstorlekar bland Teknikföretagens medlemmar. Det finns således både små företag som är att klassa som digitala ledare, och stora företag som upplever att de släpar efter. (Se figur.) Orsakerna till skillnaderna i mognadsgrad är mångfacetterade och sträcker sig från organisation och ledarskap till prioriteringar och kompetensbrist. Det är dock inte enbart en fråga som är avhängigt antal anställda.

Figur 2. Hur är statusen på digitaliseringsarbetet?
Digital mognadsgrad bland Teknikföretagens medlemmar, 2025

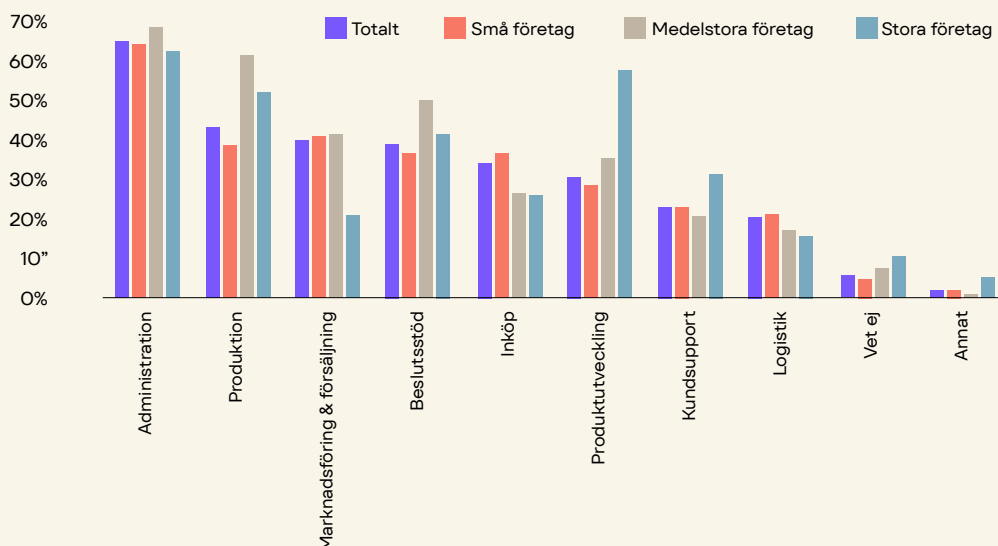


Digitaliseringens påverkan på teknikindustrin

Den digitala tekniken kan användas på flera sätt och fungerar i det närmaste som en verktygslåda och en innovationsplattform för Teknikföretagens medlemmar. Hela företagens verksamhet kan förändras, förstärkas och förbättras med hjälp av den digitala tekniken. Alla delar av verksamheten påverkas, dock inte i lika stor utsträckning vid varje given tidpunkt.

I nuläget förefaller digitalisering ha störst inverkan på hur administrativa uppgifter och processer utförs. Här pekar företagen på att den digitala tekniken underlättar allt från efterlevnad av regler och lagar till hantering av beställningar och fakturering påverkas av digital teknik. Det är också påtagligt att mindre företag ser ökade möjligheter att förändra marknadsföring, försäljning och inköp genom digitalisering, medan deras medelstora motsvarigheter synbart framhåller att beslutsfattande och produktionsprocesser påverkas. För stora företag är tonvikten istället på produktutveckling, där den digitala tekniken har påtagliga konsekvenser för design och framtagning av nya och förbättrade produkter. (Se figur).

Figur 3. Vilka områden påverkas mest av digitaliseringen?
Identifierade områden där Teknikföretagens medlemmar bedömer att digital teknik kommer att få störst påverkan på verksamheten (hur arbetet utförs) under de närmaste fem åren (2025-2030)



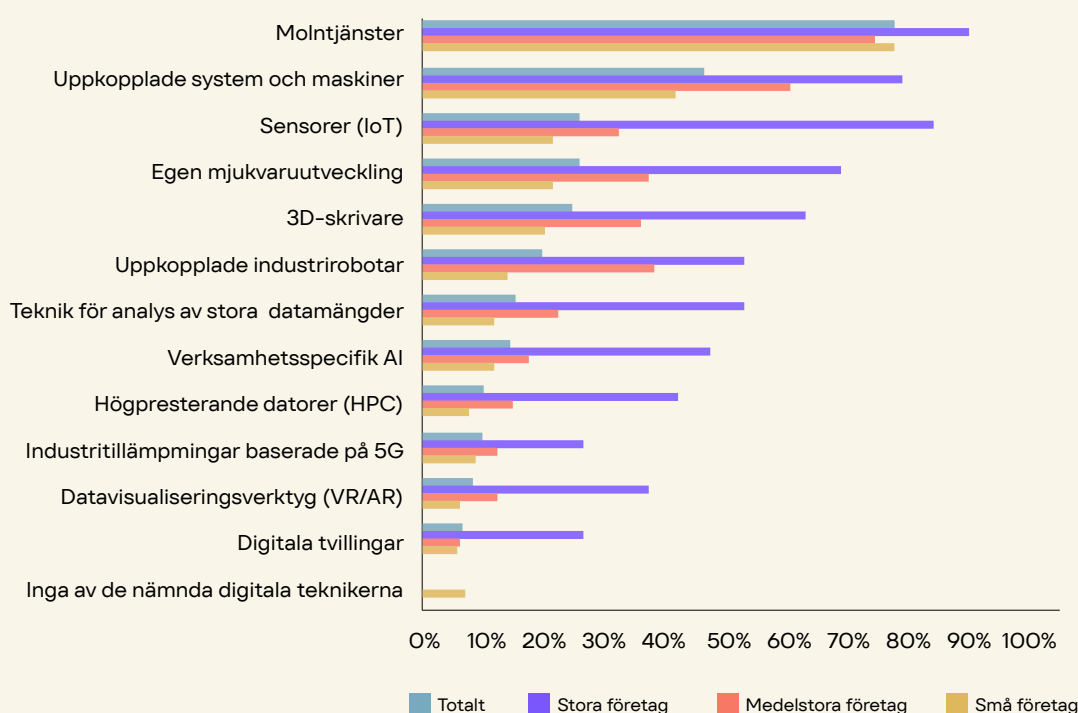
Användningen av digital teknik inom teknikindustrin

På samma sätt som digitalisering är begreppet digital teknik mångtydigt. Det rymmer en rad ömsesidigt förstärkande tekniker som förändras och omformas över tid. Variationen, både i tillgång och användning av den digitala tekniken, är emmertid påtaglig. Det kan dock konstateras att en väldigt stor del av Teknikföretagens medlemmar (nära 80 procent) nu använder olika typer av molntjänster – det vill säga digitala tjänster som kan tillhandahållas över nätet. Det är även vanligt med olika lösningar för att koppla upp maskiner och utrustning lokalt. En något mindre andel, ca 25 procent av de tillfrågade medlemsföretagen, uppger därtill att de använder mer avancerade tillämpningar som uppkopplade sensorer (IoT), har egen mjukvaruutveckling samt utrustning för 3D-printing (additiv tillverkning) i sin verksamhet.

Skillnaden i användning av digital teknik är dock markant om hänsyn tas till företagsstorlek. Generellt sett så använder större företag flera olika digitala tekniker och har mer avancerade tillämpningar. Ett exempel är AI där nära hälften av de större företagen uppger att de har verksamhetsspecifika tillämpningar mot runt 15 procent för de mindre och medelstora. (Se figur).

Figur 4 Vilken digital teknik används inom industrin?

Användning av digitala tekniker bland Teknikföretagens medlemmar, 2025



Användning av AI inom teknikindustrin

Utöver de företag som uppger att de infört och använder verksamhetsspecifik AI, så finns en påtagligt större grupp som experimenterar med tekniken.

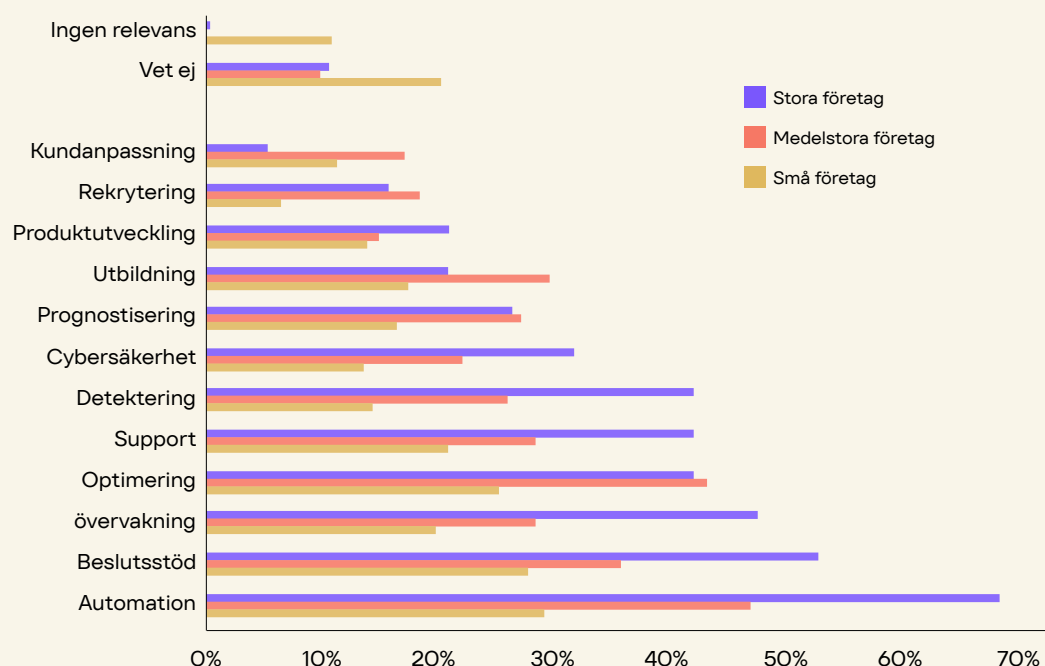
Totalt sett handlar det om ca 25 procent av de mindre företagen, nästan 60 procent av de medelstora företagen och ca 75 procent av de stora företagen. Andelarna indikerar att aktiviteten och intresset för AI är påtagligt högt inom hela teknikindustrin och att det finns en förhållandevis stor grupp som har projekt för att möjliggöra eller testa verksamhetsanpassade AI-tillämpningar (även om inte alla infört tekniken i skarpt läge).

Vad som är prioriterade tentativa tillämpningsområden varierar, men sammantaget är förhoppningarna kring vad AI kan åstadkomma stora bland Teknikföretagens medlemmar. Generellt uppfattas AI som en generisk teknik och ett viktigt byggblock för att realisera förbättringar inom ett stort antal områden. Tillämpningsområden inkluderar framför allt produktionsnära verksamheter som automation, beslutsstöd, övervakning och optimering samt att kunna upptäcka och undvika avbrott och störningar. Det handlar till stor del om tillämpningar med gemensam nämnare i att de ger direkt mätbar ekonomisk nytta.

Det är också tydligt att det finns en skillnad i synen på AI mellan företag baserat på storlek. Stora företag ser generellt fler tentativa tillämpningar med AI medan en ansevärd andel mindre företag (ca 20 procent) svarar att de inte vet. Utöver dessa finns därtill ca 10 procent av småföretagen som uppger att AI-teknik är helt irrelevant för deras verksamhet och att de därför inte är intresserade av tekniken. (Se figur).

Figur 5. Till vad kan AI användas?

Relevanta användningsområden för Teknikföretagens medlemmar, 2025



Hur används AI idag?

– exempel från Teknikföretagens medlemsföretag

1. Produktionsoptimering

Genom bildigenkänning och maskininlärning kan AI upptäcka defekter i produkter snabbare och mer noggrant än manuella inspektioner, vilket höjer kvaliteten och minskar produktionsfel.

2. Prediktivt underhåll

Genom AI-driven analys av sensordata kan företag förutse maskinhaverier och optimera underhåll. Detta minskar stilleståndstider och ökar livslängden på utrustning.

3. Automatiserad design och utveckling

AI används för att effektivisera och förbättra designprocesser inom teknikindustrin. Genom generativ design och AI-driven simulering kan företag snabbare utveckla och optimera produkter, minska materialåtgång och förbättra prestanda.

Exempel på företag med verksamhetsspecifika AI-tillämpningar:

ABB: Integrerar AI-programvara i sina system, vilket möjliggör förbättrad och mer avancerad kvalitetsinspektion.³

AB Volvo: Använder transportrobotar med AI för att förbättra samarbete mellan robotar och människor i tillverkning av lastbilar.⁴

Ericsson: Tillämpar maskininlärning och avancerad analys för automatiserad problemlösning och optimerad nätverksprestanda.⁵

GKN Aerospace: Producerar säkerhetskritiska delar till flygmotorer med hjälp av additiv tillverkning (3D-printing) och använder AI för att kontrollera att processen uppfyller specifikationerna.⁶

Sandvik: Använder AI för att förenkla användargränssnitt i tillverkningsprocesser så att mer informerade beslut kan göras.⁷

Saab: Använder AI för att kunna designa om och därmed förbättra egenskaper hos sina produkter.

Volvo Cars: Använder AI som stöd i mjukvaruutveckling vilket höjer produktiviteten och kvaliteten på programkoden som används i företagets produkter.

³ ABB, "ABB riding the wave", <https://new.abb.com/news/detail/113078/abb-riding-the-wave-of-industrial-ai-innovation>

⁴ AB Volvo "AI", <https://www.volvogroup.com/en/news-and-media/news/2024/nov/ai-modern-manufacturing.html>

⁵ Ericsson, "Automatic hybrid AI", <https://www.ericsson.com/en/blog/2024/6/improved-network-fault-handling-with-hybrid-ai?>

⁶ IT-finans, "Fokus på AI och digitalisering i flygindustrin", <https://it-finans.se/civilminister-erik-slottner-besoker-gkn-aerospace/>

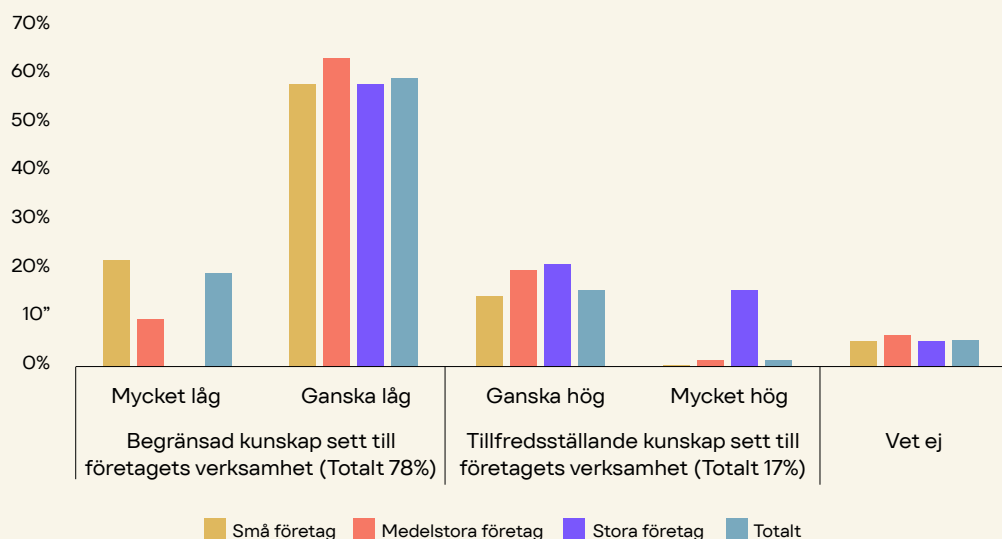
⁷ Sandvik, "Sandvik AI investments", <https://www.home.sandvik/en/stories/articles/2025/Q2/ai-investments-is-paying-off/>

Kunskapen kring AI inom teknikindustrin

Trots den höga aktivitetsgraden runt AI och de stora förhoppningarna om teknikens tillämpningsområden så finns det fortsatt förbättringspotential vad gäller att förstå hur tekniken kan komma till reell användning. Hos den stora majoriteten av Teknikföretagens medlemmar är kunskapen runt AI relativt låg. Det gäller oavsett storleksklass. Nästan 80 procent bedömer att deras egen kunskap, med hänsyn tagen till företagets verksamhet, är begränsad. Omvänt är det i princip endast de större företagen som bedömer sin egen kunskap inom AI som mycket hög. Detta indikerar att det finns ett fortsatt stort kunskapsunderskott inom industrin med avseende på AI, vilket inte är konstigt med tanke på att tekniken haft en snabb utveckling och att innovationstakten är fortsatt hög med en ström av nya tillämpningar och banbrytande lanseringar. (Se figur).

Figur 6. Hur är kunskapsläget om AI?

Bedömning av den egna kunskapen om AI sett till företagets verksamhet bland Teknikföretagens medlemmar, 2025



Ett exempel på utvecklingsprång inom AI är Deepseeks lansering i början av 2025. Företaget presenterade då en AI-modell baserad på öppen källkod som uppfattas som både kraftfullare och mer resurseffektiv än etablerade modeller på marknaden. Denna innovation kan göra avancerade AI-funktioner mer tillgängliga på enheter med lägre prestanda, såsom stationära datorer, laptops och mobila enheter, vilket skapar ökad flexibilitet kring hur AI-lösningar kan tillämpas.⁸

⁸⁾ Forbes, "Deepseeks AI innovation", <https://www.forbes.com/sites/garthfriesen/2025/01/29/deepseeks-ai-innovation-what-it-means-for-investors-and-big-tech/>

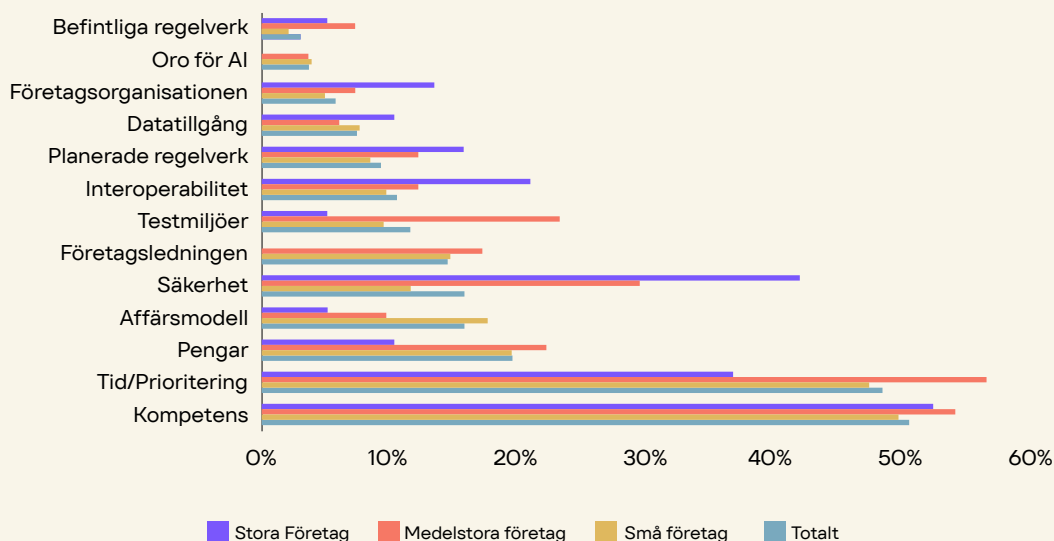
Hinder för AI tillämpningar

Den snabba utvecklingen av AI och den begränsade kunskapsnivån som detta medför kommer också till uttryck ifråga om hinder för initiering eller uppskalning av tekniken bland Teknikföretagens medlemmar. Från företagets perspektiv gör en bristande tillgång till personer som har verksamhetsnära kunskap inom AI att investeringar hålls tillbaka. Trots omfattande "hype" kring tekniken är det därtill inte självklart för företagen att AI-tillämpningar kan eller ska prioriteras. Andra projekt och aspekter av verksamheten bedöms som mer betydelsefulla, varför AI-projekt inte kan ges obegränsat med resurser i form av vare sig tid eller pengar. Andra hinder på vägen mot ökad AI-användning är säkerhetsaspekter, där inte minst medelstora och stora företag ser säkerhetsutmaningar i fråga om lagring av data, tilliten till resultaten och robustheten i befintliga AI-system.

Som tillägg kan det också konstateras att de större företagen (som generellt har kommit längre i arbetet med AI än de små och medelstora företagen) har en mer sammansatt bild av utmaningarna för implementering. De ser sammantaget fler hinder på vägen till fullt integrerad AI-användningen än deras motsvarigheter med färre anställda. (Se figur).

Figur 7. Vad står i vägen för AI-användningen?

Identifierade primära hinder för att initiera, öka satsningar eller skala upp verksamhetsspecifika AI-tillämpningar hos Teknikföretagens medlemmar, 2025



Strategiska områden för teknikindustrin

Även om stort fokus är på AI så är det viktigt att komma ihåg att det finns en rad digitala tekniker som kan realisera nyttoeffekter, både i form av ökad produktivitet i produktionen, men också i syfte att bidra i omställning till cirkulära affärsmodeller, högre motståndskraft mot störningar (resiliens) och en högre grad av innovationskraft. För flertalet av Teknikföretagens medlemsföretag är det således viktigt att säkerställa kontinuerliga investeringar i flera olika digitala teknikområden. Av strategisk betydelse för den framtida konkurrenskraften bedöms i nuläget nedan listade digitala områden vara – både enskilt och tillsammans. Områdena, som inkluderar AI, ses som ömsesidigt förstärkande och det påtalas att styrkan ligger i att kunna kombinera dem sömlöst och robust.

- **Industriellt tillämpad Ai**
Applikationer med fysisk anknytning samt effektivisering och automatisering av processer och arbeten.
- **Konnektivitet**
Säker, stabil uppkoppling och dataanalys.
- **Elektronik**
Halvledare, kraftelektronik, sensorer och elektroniska system.
- **Mjukvaruutveckling**
Industriell mjukvaruutveckling, vilket behöver kombinera storskalighet, snabbhet, kvalitet och säkerhet för produkter som ofta är i ett cyberfysiskt sammanhang.
- **Cybersäkerhet**
Skydd av industriella system och produkter samt tillhörande lösningar för att förebygga och hantera digitala hot och attacker.
- **Systemintegration**
Interoperabilitet mellan olika system och aktörer samt sammankoppling av delar (hårdvara, mjukvara, data och processer) till en helhet (komplexa system och "system av system").

En ytterligare aspekt som framhålls av Teknikföretagens medlemmar är att den digitala tekniken behöver kunna verksamhetsanpassas. Det innebär bland annat att utveckling, test, uppskalning och implementering av digital teknik behöver ske i nära samklang med andra teknikområden där industrin i Sverige har en styrkeposition. Det inkluderar bland annat:

- **Produktionstekniker**
Automation, robotik och mekanik.
- **Framdrivningstekniker**
Batterier, vätgas, bränsleceller och andra fossilfria bränslen.
- **Tekniker för energisystem**
Infrastruktur för lagring, överföring, laddning och generering av fossilfri energi.
- **Tekniker för bearbetning av mineraler, metaller och polymerer**
Avancerade och förbättrade materialegenskaper i de cirkulära materialflödena.

Cyberhotet mot teknikindustrin

Digitaliseringen kommer dessvärre inte bara med möjligheter. Det försämrade omvärldsläget har förvärrat en redan utmanande situation i frågan om digital säkerhet. Det märks på flera sätt, däribland att cyberattacker mot Sverige har ökat. Ökningen var under 2024 störst i hela Europa.⁹ Attackerna har också systematiserats och blivit mer professionella. Det innebär att teknikindustrin i Sverige idag kan uppfattas som ett prioriterat mål. Säkerhetspolisen uppger därtill att antalet uppkopplade enheter som kapats och fjärrstyrs för attacker uppgår till 10 000, vilket är en hög siffra i internationell jämförelse.¹⁰ Kostnaderna för cyberattacker uppskattas på årsbasis till miljardbelopp.¹¹

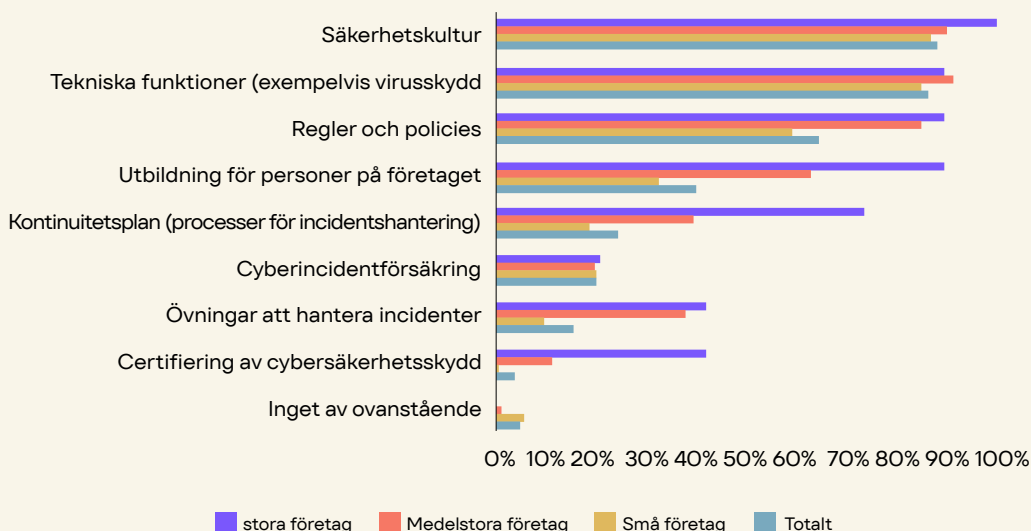
En försvårande omständighet är att attackerna som riktas mot svensk teknikindustri i ökad utsträckning kommer från statsunderstödda aktörer som vill stjäla teknologi, affärskänslig data och immateriell egendom. Därtill är processer och system inom automation och produktion en måltavla hos företag oavsett storlek. Industrins transformation från lokalt avgränsade enheter, till uppkopplade och fjärrstyrda system skapar sårbarheter som utnyttjas av antagonister.

Cybersäkerhet inom teknikindustrin

Den nya situationen har inte undgått teknikindustrin. För Teknikföretagens medlemsföretag har cybersäkerhet¹² varit en angelägen fråga under flera år. Följaktligen är elementärt cyberskydd i dagsläget utbrett bland stora såväl som mindre företag. Nästan 90 procent av de tillfrågade företagen uppger att de idag har en "säkerhetskultur" – det vill säga att det finns en medvetenhet bland ledning och anställda om risken för att digitala angrepp och incidenter kan drabba verksamheten. Det gör företagen mer vaksamma. De flesta företag använder också olika tekniska funktioner såsom virusskydd, brandväggar och automatiska uppdateringar för att öka sin digitala säkerhet. Samma sak gäller för regler och policies. Vägledningar kring handhavande med digitala system exempelvis för programvara, utrustning och användarbehörigheter är utbredd praxis hos en majoritet av företagen. Det löser inte allt men skapar ökad tydlighet kring vad som gäller och förväntas. (Se figur).

Figur 8. Finns det något cyberskydd?

Andel som vidtagit olika typer av åtgärder för att förebygga och skydda mot cyberattacker bland Teknikföretagens medlemmar, 2025



⁹ Check Point Research, "Cyberattacker ökar med 165 procent i Sverige – största ökningen i Europa", <https://www.voister.se/artikel/2024/10/cyberattacker-mot-sverige-okar-mest-i-europa/>

¹⁰ Säkerhetspolisen, "Årsbok 2023/2024", <https://sakerhetspolisen.se/download/18.5cb30b118d1e95af-fec371708502268494/L%C3%A4gesbild%202023-2024.pdf>

¹¹ Teknikföretagen, "Cyberhoten", <https://www.teknikforetagen.se/globalassets/rapporter-publikationer/digitalisering/cyberhoten-sa-ser-hotbilden-och-attackerna-ut-mot-svenska-teknikforetag.pdf?43WC0d>

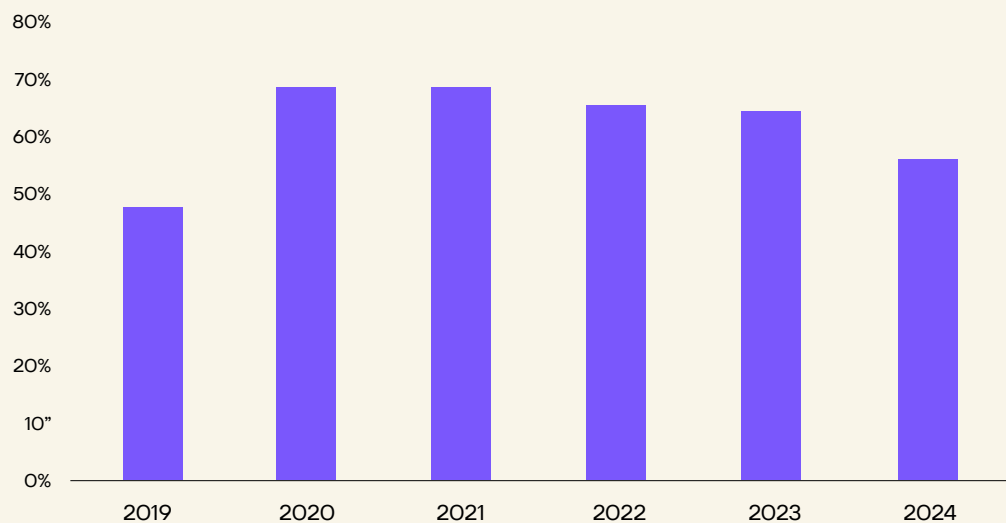
¹² Cybersäkerhet innebär i den här kontexten skydd mot att någon medvetet vill förstöra eller stjäla information.

Cyberattacker mot teknikindustrin

Det systematiska arbetet förefaller också ha gett resultat. Detta indikeras av att en fallande andel av Teknikföretagens medlemsföretag identifierat cyberattacker. Andelen har successivt sjunkit från nästan 70 procent 2020 till ca 55 procent 2024.¹³ Utvecklingen bör tolkas med försiktighet. Frågan är känslig och andelen som uppger att de inte vet om de drabbats kan rymma ett mörkertal.¹⁴ Eftersom det inte finns några tecken på att volymen av cyberattacker minskat mot mål i Sverige är en tentativ förklaring att attackerna inte enbart minskat utan att de också blivit mer sofistikerade och utförda på ett mer professionellt sätt – vilket gör de svårare att upptäcka med konventionella metoder. (Se figur)

Figur 9. Är cyberattacker en utmaning?

Andel av teknikföretagens medlemmar som identifierat cyberattacker under det senaste året, 2019–2024



Bland de företag inom teknikindustrin som utsätts för cyberattacker är digitala bedrägeriförsök (phishingattacker) vanligast följt av nedsmittning med elakartad programkod i form av virus och trojaner. Attackerna kan också samvariera och vara beroende av varandra, det vill säga ett digitalt bedrägeriförsök kan resultera i att företag blir utsatta för utpressningsförsök eller att någon försöker använda stulna uppgifter i syfte att manipulera digitala system och utrustning. I de flesta fall sker ingen polisanmälan hos de företag som blir utsatta.¹⁵

Utöver attacker från externa aktörer förekommer det att personer på företagen själva agerat på ett sätt som oavsiktligt lett till exempelvis driftsavbrott av digitala system eller att data spridits till obehöriga. Det kan exempelvis begås fel vid konfigurering av en server eller en brandvägg, vilket kan leda till att system blir otillgängliga eller att obehöriga får åtkomst. På samma sätt kan viktiga filer delas på publika tjänster med begränsad säkerhet eller raderas utan att säkerhetskopiering gjorts. Denna typ av incidenter förekommer men är förhållandevis ovanliga. Totalt sett är det under 5 procent av de tillfrågade företagen som anger att de känner till att sådana incidenter förekommer hos dem. Det kan emellertid noteras att andelen är påfallande högre för större företag. (Se figur nästa sida).

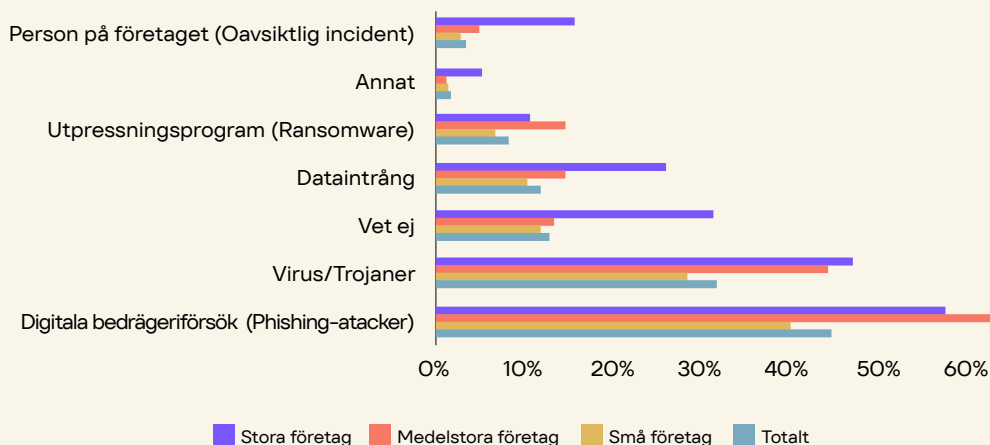
¹³ Data är inte helt jämförbara över tid då uppfattningen om vad som utgör en cyberattack förändrats

¹⁴ Exempelvis uppger 30 procent av de större företagen "vet ej" på frågan om de identifierat cyberattacker under det senaste året.

¹⁵ Uppgifter från Polismyndigheten göra också gällande att cyberattacker mot näringslivet kategoriskt underskattas på grund av en underrapportering från de företag som drabbas.

Figur 10. Vilken typ av cyberattacker har identifierats?

Typ av identifierade cyberattacker mot Teknikföretagens medlemmar under 2025

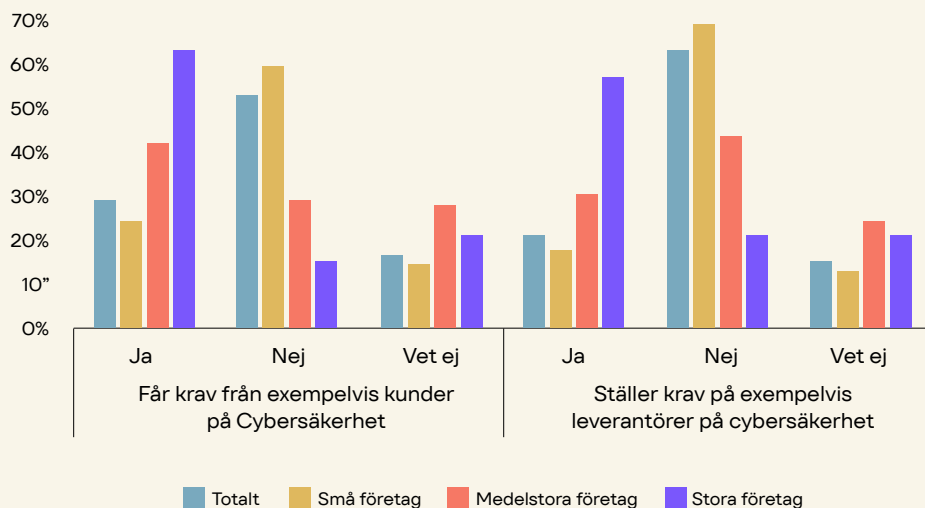


Krav på cybersäkerhet inom teknikindustrin

Eftersom företagen är sammankopplade i leverantörskedjor är deras cyberskydd ömsesidigt beroende. En viktig del i arbetet för att förbättra det digitala skyddet är därför kravställning. I nuläget är det emellertid en relativ begränsad andel av företagen som ställer krav (ca 20 procent) eller har krav på sig (ca 30 procent). Lägst är kravbilden hos mindre företag – medan de större både har krav från exempelvis kunder och ställer krav på sina leverantörer. Eftersom mindre företag ofta är underleverantörer till större företag indikerar svaren att kravbilden tillämpas selektivt, alternativt att kunskapen om de krav som faktiskt finns inte genomsyrar leverantörsledet i önskvärd omfattning. Svaren står också i motsättning till det faktum att företagen (oavsett storlek) unisont uppger att de har en säkerhetskultur.¹⁶ (Se figur).

Figur 11. Ställs krav på cybersäkerhet?

–Andel bland Teknikföretagens medlemmar som har krav (från exempelvis kunder) respektive ställer krav (på exempelvis leverantörer) kring cybersäkerhet, 2025



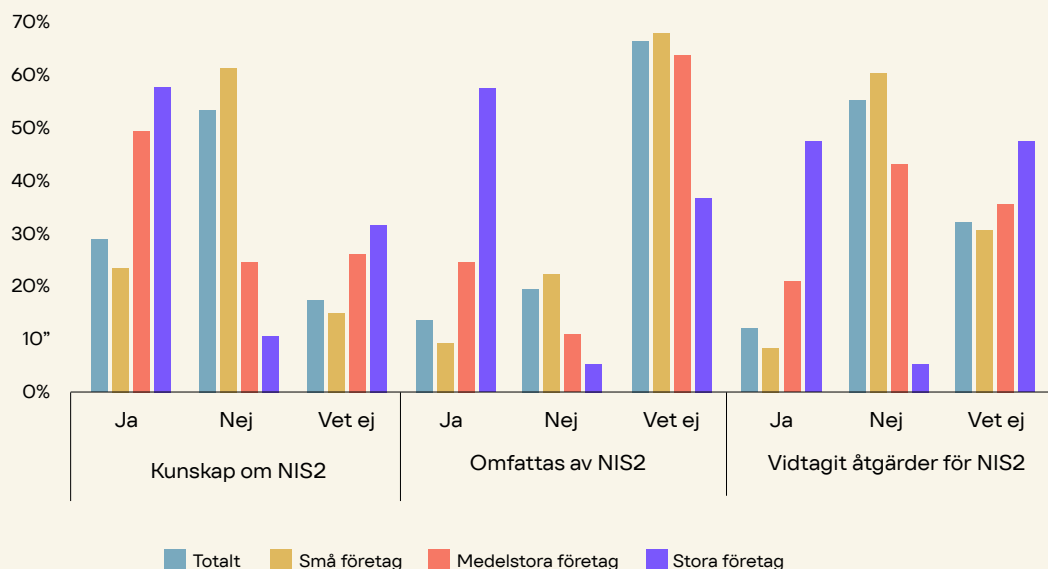
¹⁶⁾ Med säkerhetskultur avses att det finns en medvetenhet bland ledning och anställda om risken för att digitala angrepp och incidenter kan drabba verksamheten.

Lagstiftning om cybersäkerhet

Utöver frivillig kravställning håller omfattande tvingande lagstiftning på att introduceras. Detta inkluderar bland annat en ny lag för att uppnå en högre gemensam cybersäkerhetsnivå. Fler branscher berörs, däribland teknikindustrin. Lagen baseras på ett direktiv från EU kallat NIS2 och ställer tydligare krav på bland annat riskanalyser och olika säkerhetsåtgärder. Lagen är försenad, men förväntas träda i kraft under våren/sommaren 2025. Bland företagen är emellertid kunskapen om lagen påtagligt begränsad, liksom insikten om vilka som omfattas samt om åtgärder vidtagits. Det är en utmaning eftersom företag som inte lever upp till lagens intentioner kan drabbas av höga vitesbelopp. I juridisk mening har cybersäkerhet blivit en ledningsfråga.¹⁷ (Se figur).

Figur 12. Finns kunskap om cybersäkerhetslagstiftning?

Andel av Teknikföretagens medlemmar som känner till, omfattas och vidtar åtgärder med anledning av cybersäkerhetslagen NIS2.



NIS2-lagen är endast en av flera nya lagar som nu introduceras på cybersäkerhetsområdet. Högre krav på processer och dokumentation har för avsikt att höja lägsta nivån på de digitala systemen. I praktiken kommer det också med administrativa kostnader. Kunskapen om dessa kostnader omgärdas i nuläget av viss osäkerhet hos Teknikföretagens medlemmar, totalt sett saknar 35 procent kunskap. Av de som kan svara uppger i nuläget drygt hälften att kostnaderna bedöms vara hanterbara. Med detta avses att kostnaderna som lagstiftningens krav ställer är betydande, men i förhållande till nyttan inte ett oöverstigligt hinder för digitaliseringsarbetet och de investeringar detta kräver.

¹⁷⁾ NIS2 föreskriver ett högsta bötesbelopp på minst 7 000 000 EUR eller minst 1,4 procent av den totala globala årsomsättningen under föregående budgetår, beroende på vilket som är högst. EC, Direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet), Direktiv - 2022/2555 - EN - EUR-Lex.

Rekommendationer för att stärka teknikindustrins digitalisering

För att sammanfatta ovanstående kan det konstateras att digital teknik har en genomgripande påverkan på teknikindustrin i Sverige. Digitaliseringen genererar stora möjligheter, men innebär även många utmaningar. Det finns dock inget som tyder på att utvecklingen av digital teknik kommer att avta eller i praktiken gå att välja bort. Att med hjälp av exempelvis AI kunna samla, aggregera, analysera och extrahera data är nästan en förutsättning för bibehållen konkurrenskraft. Detta kommer i sin tur ställa krav på omfattande förmåga att digitalt säkra produkter och produktion, samt bygga motståndskraft mot störningar och attacker.

För det enskilda företaget är digitalisering en ledningsfråga så till vida att det i grunden påverkar hur verksamheten ska utföras och vilka investeringar och kompetensuppbyggnad som är önskvärda att göra för att kunna hänga med i utvecklingen. Därtill kommer ett formellt ansvar genom de krav som finns genom lagar som exempelvis NIS2. Inget enskilt företag kan i juridisk mening fränsäga sig ansvar.

För att bistå behöver företagen:

- Kunna erbjudas stöd och konsultation i uttolkning av de lagkrav som ställs upp av myndigheterna i Sverige och på europeisk nivå. Det är väsentligt att myndigheter så som länsstyrelsen kan ge vägledning och är beredda att kunna besvara frågor kring hur lagar ska tolkas och omsättas.
- Ges möjlighet att delta i ett digitaliseringslyft för att öka baskunskapen hur digital teknik kan användas och integreras samt hålla jämna steg med utvecklingen inom bland annat konnektivitet, AI och cybersäkerhet. Här finns synnerligen goda erfarenheter att hämta från Tillväxtverkets arbete inom smart industri exempelvis Robotlyftet.¹⁸
- Få ökad tillgång till relevant kompetens, inte minst personer som har verksamhetsnära kunskap inom AI. Här spelar lärosätena i allmänhet och RISE i synnerhet en central roll för att säkerställa att forskning och utveckling kan nyttiggöras.

¹⁸⁾ Tillväxtverket, "Smart industri", <https://tillvaxtverket.se/tillvaxtverket/guiderochverktyg/exempelfranverkligheten/exempelfranverkligheten/starkdinverksamhetmedautomationochrobotisering.2936.html>

För teknikindustrin som helhet är det på motsvarande sätt viktigt att digital teknik prioriteras i den nationella politiken för att främja innovation. Strategiska områden av vikt för industrin, så som elektronik, konnektivitet och mjukvaruutveckling är särskilt angeläget att investera resurser i. Ett sätt att göra detta är via riktade insatser som bygger på samarbete mellan företag, industri, institut och akademi. Teknikföretagen förespråkar ökad forskningssamverkan, bland annat genom förstärkning av programmet Avancerad Digitalisering och Net Zero Industry – två strategiska innovationsprogram som syftar till att samla kompetenser och hitta lösningar på gemensamma industriella utmaningar där digital teknik utgör kärnan.

Ur Teknikföretagens perspektiv krävs också goda möjligheter att testa och utvärdera digitala lösningar, särskilt för att säkerställa en adekvat skyddsnivå –det vill säga funktioner för att förhindra, hantera och minimera konsekvenserna av digitala attacker och störningar. Tillgång till testanläggningar är därför väsentliga att säkerställa. Här spelar forskningsinstitutet RISE en viktig roll som unik brygga mellan lärosäten och företag.



Bilaga

Nyckelbegrepp som förekommer i rapporten

Artificiell Intelligens (AI)

Med AI avses här datorsystem inklusive program och tillämpningar som efterliknar mänskligt beteende och tänkande. Med detta menas att datorsystemen lär sig, är medvetna om sin omgivning och vidtar åtgärder som maximerar chanserna att lösa specifika uppgifter. Systemen kan med andra ord lära sig nya saker på egen hand (utan mänsklig inblandning) och ständigt bli bättre. Detta är en väsentlig skillnad från traditionella system som enbart gör exakt det som de blivit programmerade för. AI-tillämpningar som är utvecklade eller anpassade för ett företags verksamhet kallas verksamhetsspecifika.

Cybersäkerhet

Cybersäkerhet definieras som all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot. Definitionen inkluderar informationssäkerhet, it-säkerhet, ot-säkerhet och leveranskedjesäkerhet. Ett närliggande begrepp är också digital resiliens som tydligare understryker att de elektroniska systemen ska klara påfrestringar och störningar.

Cyberattacker

Med cyberattacker avses här digitala attacker mot enskilda personer eller grupper som angriper datorsystem och processer för att stjäla affärskänslig information, utpressa användare, störa processer eller förstöra data. Cybersäkerhet är en delmängd av begreppen informationssäkerhet och IT-säkerhet.

Digitalisering

Med digitalisering avses i denna undersökning primärt industriell digitalisering det vill säga att produkter, processer och system kopplas upp och kopplas ihop samt att data kan utvinnas och analyseras för att generera nytta. För att kunna möjliggöra digitaliseringen behövs digitala tekniker.

Digitala tekniker

Digitala tekniker är ett samlingsnamn som täcker in många olika informations- och kommunikationstekniker bland annat radioteknik, uppkopplade robotar, sensorer och artificiell intelligens (AI).

Digital mognad

Med digital mognad avses att företag har god förståelse av den digitala tekniken, hur den kan tillämpas och också använder den på ett ändamålsenligt sätt.



Teknikföretagens 4500 medlemsföretag står för en tredjedel av Sveriges export och över en miljon jobb. Vår uppgift är att stärka våra medlemmars konkurrenskraft och driva den hållbara utvecklingen framåt. Tillsammans med företag över hela landet formar vi teknikbranschens framtid – för vi är tekniksverige.

Pulicerad: April 2025

www.teknikforetagen.se