

CIO ANALYTICS

NORDEUROPAS STÖRSTA RAPPORT FÖR IT-BESLUTFATTARE

18 %

har skapat
betydande värde
med AI.

76 %

övar inte sina
beredskapsplaner
regelbundet.

2026

SVERIGE

Nr. 1

största utmaning
för it-beslutfattare:
resurser.

DJUPINTERVJUER

16

Pite Energi:

Det yttersta säkerhetsansvaret
ligger hos ledningen.

22

Bastard Burgers:

AI måste driva affärsnytta
– inte bara teknisk innovation.

34

Falu kommun:

Utan it-investeringar kan
verksamheten inte fungera.

Sida #

Innehåll



Om rapporten

CIO Analytics är en årlig, datadriven undersökning som är utformad för att fånga prioriteringar, utmaningar och strategisk inriktning hos dagens it-beslutsfattare. Undersökningen lanserades först i Sverige 2018 och har sedan dess utvecklats till en av de mest heltäckande studierna av it-ledarskap i Nordeuropa.

År 2024 utökades undersökningen till att även omfatta Norden och de baltiska länderna, för att skapa ett bredare perspektiv (som i rapporten benämns Nordeuropa). Undersökningen riktar sig till CIO:er och it-beslutsfattare inom både privat och offentlig sektor.

2026 års upplaga bygger på 1 478 svar, varav 59 procent från privat sektor och 41 procent från offentlig sektor, vilket ger en robust grund för benchmarking, trendanalys och strategiska insikter.

Data och diagram i den här rapporten baseras på undersökningssvaren. För tydlighet och konsekvens har vissa frågor och svarsalternativ anpassats något, samtidigt som den ursprungliga avsikten och betydelsen har bevarats.

Rapporten ges ut av Atea ASA, den ledande leverantören av it-infrastruktur i Norden och Baltikum.

Ta del av fler insikter och ladda ner rapporten.



- 4 KAPITEL 1: IT-LEDARSKAP I EN SNABBFÖRÄNDERLIG VÄRLD**
- 5 Den moderna it-beslutsfattaren ser hela bilden
- 6 Verksamhetskrav gör att säkerhet fortsatt står i centrum
- 7 Drivkraften är transformation, inte nödvändiga åtgärder
- 8 Den växande belastningen bakom it-avdelningarnas dagliga arbete
- 9 **I fokus:** En balansakt mellan acceleration och ansvar

- 10 KAPITEL 2: REDO FÖR NUET, RUSTAD FÖR MORGONDAGEN**
- 11 Högre mognadsgrad synliggör fler risker
- 12 Därför är säkerhetsarbetet svårare än det borde vara
- 13 Incidenter driver aktivitet men skapar inte immunitet
- 14 De flesta planer är oprövade när det verkligen gäller
- 15 Säkerhetsarbetet anpassas efter omvärldsläget
- 16 **I fokus:** På Pite Energi ligger det yttersta säkerhetsansvaret hos ledningen

- 17 KAPITEL 3: FRIGÖRA VÄRDET: FRÅN UTFORSKARE TILL UTÖVARE**
- 18 Från assistenter till agenter: nästa fas i AI-användningen
- 19 Svårt att gå från experiment till genomförande
- 20 Värdeskapandet med AI ökar långsamt trots snabb mognad
- 21 Många organisationer inför AI utan en mätbar strategi
- 22 **I fokus:** AI måste driva affärsnytta – inte bara teknisk innovation

- 23 KAPITEL 4: FÖRÄNDRADE PERSPEKTIV PÅ MOLN OCH HÅLLBARHET**
- 24 Från optimism till neutralitet: attityderna till publika molntjänster förändras
- 25 Strategi snarare än teknik styr tilliten till molntjänster
- 26 När prioriteringar förändras riskerar hållbarhet att hamna i skymundan
- 27 Högpresterande team uppstår inte av sig själva
- 28 **I fokus:** SEB bygger högpresterande team genom tydlighet och mångfald

- 29 KAPITEL 5: SKAPA UTRYMME FÖR DET SOM SPELAR ROLL**
- 30 It-utgifterna ökar men prioriteringarna förändras
- 31 Kompetensutveckling, partnerskap och AI formar framtidens kompetensbehov
- 32 It-avdelningens strategiska roll kräver nya sätt att utvärdera
- 33 Proaktiviteten ökar när it och verksamheten arbetar i samklang
- 34 **I fokus:** Utan it-investeringar kan verksamheten inte fungera
- 35 **Förberedelser för framtiden:** Lärdomar och strategier

En ny era för it-beslutsfattande

Vardagen för en it-beslutsfattare är mångfacetterad och präglas av många svåra uppgifter, där obligatoriska ansvarsområden måste balanseras mot ambitiösa mål. Rollen kräver både teknisk expertis och strategiskt tänkande. Beslut måste fattas snabbt samtidigt som flera behov konkurrerar om uppmärksamheten under ständig press.

Denna rapport baseras på en undersökning som omfattar närmare 1 500 it-beslutsfattare i Nordeuropa och djupdyker i de rådande prioriteringarna, utmaningarna och strategierna. Den belyser de mest kritiska frågorna för dagens it-beslutsfattare och beskriver väsentliga förutsättningar för ett effektivt, modernt it-ledarskap. Rapporten ger dig möjlighet att jämföra din it-verksamhet med andras, förstå trender inom säkerhet och innovation samt fatta datadrivna strategiska beslut.

Med hjälp av dataunderlaget blir rapporten ett smidigt verktyg för att förstå din och andra organisationers positionering i frågor som AI, säkerhet och resurser.

Rapporten visar även på att it-beslutsfattare blir alltmer proaktivt engagerade i organisationsstrategier. För att upprätthålla denna förändring krävs stark styrning, väldefinierade finansiella prioriteringar och tydliga förväntningar på ledarskapet. It-beslutsfattare måste också hantera utmaningar kring resursfördelning. I takt med att AI-tekniken utvecklas behöver organisationer koppla användningen av AI till konkret affärsnytta, snarare än att enbart experimentera.

Denna rapport kan hjälpa dig att bättre förstå hur teknik påverkar affärsstrategier och fungera som vägledning i din organisations pågående digitala transformation.

→ Svartsfördelning per land, av totalt 1 478 it-beslutsfattare i Sverige, Norge, Danmark, Finland och de baltiska länderna.



1 figur = 20 respondenter, avrundat till närmaste 20.

1

It-ledarskap i en snabbföränderlig värld

It-ledarskap präglas av ständiga vägval. Det här kapitlet undersöker hur it-beslutsfattare navigerar i sin roll, vad som formar sunda beslut, vad som tar mest fokus, vilka ambitioner som ökar och ledarskapsutmaningar i vardagen.

Resurser

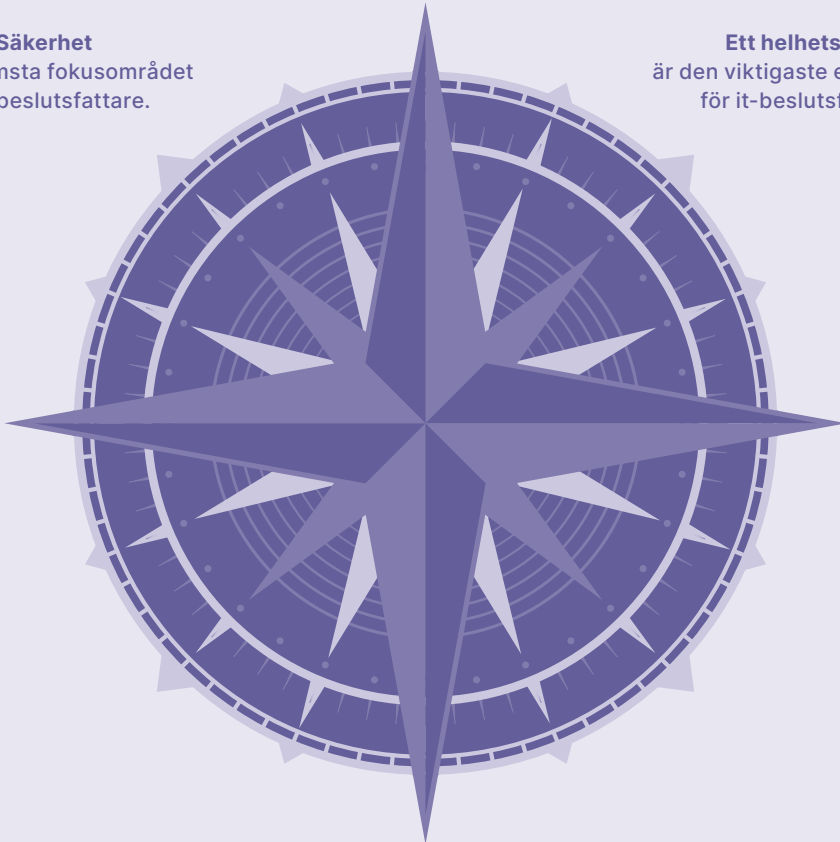
är den största utmaningen för it-beslutsfattare.

Säkerhet

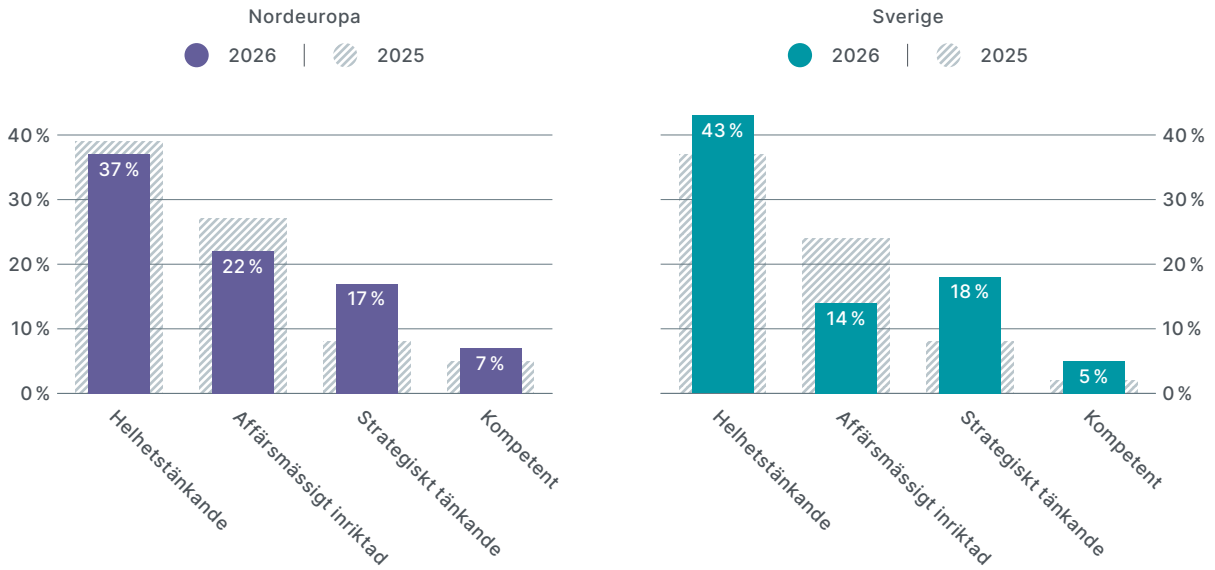
är det främsta fokusområdet för it-beslutsfattare.

Ett helhetstänk

är den viktigaste egenskapen för it-beslutsfattare.



Vad anser du vara det viktigaste kännetecknet för en bra it-beslutsfattare?



Den moderna it-beslutsfattaren ser hela bilden

En bra it-beslutsfattare kännetecknas framför allt av förmågan att se helheten. Ledare i hela Nordeuropa pekar på ett helhetsperspektiv som den absolut viktigaste egenskapen, vilket speglar att rollen numera handlar om betydligt mer än teknik. Ett helhetsperspektiv innebär att förstå hur beslut påverkar verksamheten, kostnader, risker, människor och långsiktiga resultat. Det innebär också att it behöver erkännas som en strukturell drivkraft för organisationens inriktning och inte bara en stödfunktion.

Strategiskt tänkande har blivit betydligt viktigare. Rollen skiftar från operativt överseende till långsiktiga strategier präglade av geopolitisk osäkerhet, regleringar och snabb teknisk utveckling däribland AI. Strategisk kompetens gör det möjligt för it-beslutsfattare att ta ställning i komplexa frågor och ge organisationen en riktning när förutsättningarna är oklara.

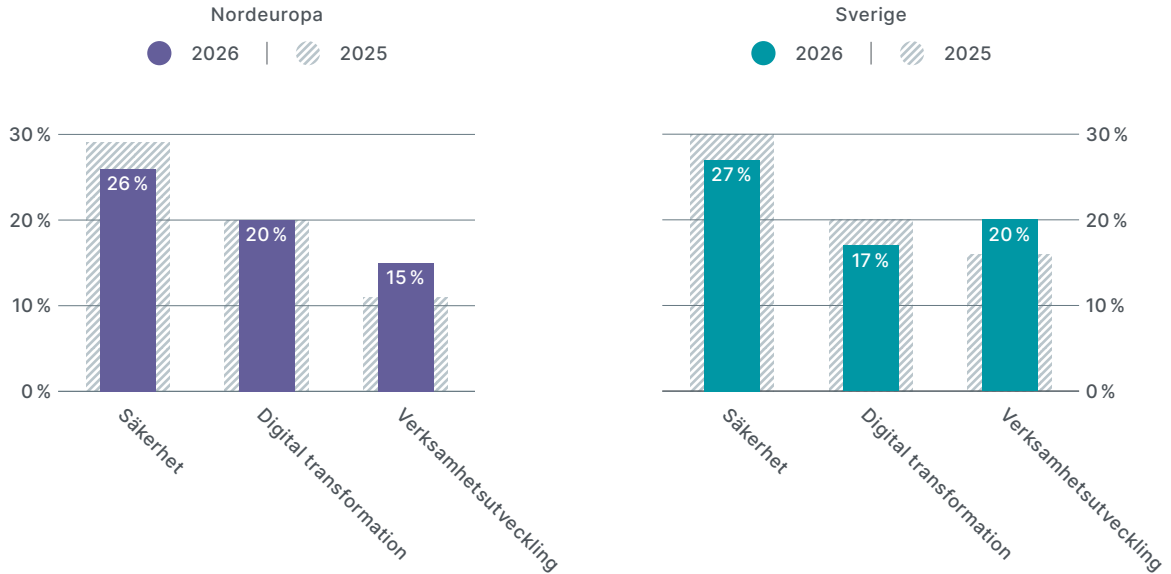
Ett starkt affärsmässigt tankesätt är viktigt i rollen. Effektiva it-beslutsfattare förstår hur teknik möjliggör tillväxt, motståndskraft och värdeskapande. De anpassar valen efter affärsmålen och vågar ifrågasätta när prioriteringar ändras.

Dessa egenskaper kännetecknar en bra it-beslutsfattare i ett modernt it-ledarskap: ett helhetstänk, strategisk förmåga och affärsinriktning. Men också mod, fokus och beslutsamhet. It-beslutsfattare agerar ofta utifrån ofullständig information, gör svåra avvägningar och balanserar höga förväntningar med ofta otillräckliga resurser. Detta gör att verksamheten i allt högre utsträckning vänder sig till it för vägledning.

Sverige i fokus

→ I Sverige anses helhetsperspektivet vara den viktigaste egenskapen hos en it-beslutsfattare. Även faktorer utanför it behöver beaktas när beslut som påverkar hela organisationen fattas. Andra viktiga egenskaper är strategiskt tänkande och att vara affärsmässigt inriktad. Betydelsen av strategiskt tänkande ökar på grund av den rådande geopolitiska situationen, medan affärs- och verksamhetsnytta är avgörande för att omvandla teknikval till konkret organisationellt värde.

Vad är ditt primära fokus i din roll som it-beslutsfattare just nu?



Verksamhetskrav gör att säkerhet fortsatt står i centrum

Sverige i fokus

→ Även om svenska it-beslutsfattare betraktar säkerhet som ett nödvändigt fokus, ofta på grund av externa faktorer och lagstiftning som påverkar deras organisationer, framgår det tydligt att säkerhet inte är det område som de helst vill fokusera på. Tvärtom minskar fokus på säkerhet från år till år, medan fokus på verksamhetsutveckling stadigt ökar.

Säkerhet är fortfarande det främsta fokusområdet för it-beslutsfattare i Nordeuropa, även om dess dominerande ställning har försvagats något. Förra året angav 29 procent säkerhet som sitt främsta fokusområde, jämfört med 26 procent i år. Trots en mindre nedgång får säkerhet fortfarande mer uppmärksamhet än något annat område. It-beslutsfattare beskriver det som ett obligatoriskt arbete drivet av regleringar, ökande hot och förväntningar på operativ stabilitet. Säkerhet fortsätter att sluka tid och resurser, även om det inte är där man tror att mest värde skapas. (Läs mer på sidorna 11-15.)

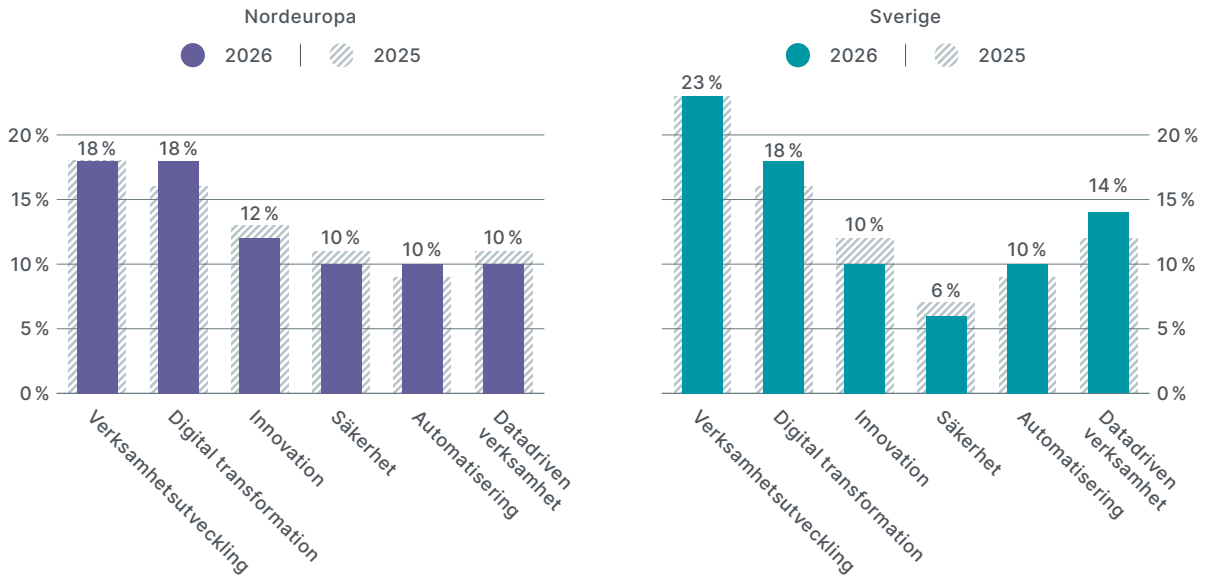
Digital transformation är fortfarande en strategisk prioritering, men konkurrerar ofta med operativa skyldigheter. När nya säkerhetskrav uppstår saktar transformationen ner. Många ser det som en återkommande trend, framsteg är möjliga men sällan kontinuerliga.

Verksamhetsutveckling hamnar på tredje plats bland de aktuella fokus-

områdena, men är ändå det område som fler it-beslutsfattare önskar att de kunde lägga mer tid på. Begränsad kapacitet och kompetensbrist gör det svårt att gå från reaktivt agerande till värdeskapande initiativ. Klyftan mellan nuvarande och önskat fokus är fortfarande en av rollens största motsättningar. (Läs mer på sidan 7.)

Organisationens storlek påverkar denna motsättning. Mindre organisationer fokuserar på överlevnad och efterlevnad. Större eller mer mogna organisationer har mer utrymme att satsa på transformation och verksamhetsutveckling. Tydliga ledningsbeslut spelar också en avgörande roll. När riktlinjer är tydliga ligger fokus på långsiktigt värdeskapande. När de är otydliga förblir it-avdelningens agerande reaktivt.

Vad skulle du vilja fokusera mer på i din roll som it-beslutsfattare?



Drivkraften är transformation, inte nödvändiga åtgärder

It-beslutsfattare i Nordeuropa uttrycker en tydlig önskan om att flytta fokus från obligatoriska operativa uppgifter till arbete som skapar långsiktigt affärsvärde. Även om säkerhet, regelefterlevnad och driftstabilitet dominerar den nuvarande agendan speglar dessa områden inte var de vill lägga mer av sin tid. Ambitionen kretsar kring verksamhetsutveckling, digital transformation och innovation. De två områden som man vill fokusera mest på har båda lyfts fram av 18 procent av respondenterna.

Klyftan mellan nuvarande och önskat fokus beror på begränsad kapacitet och otydliga uppdrag snarare än bristande vilja. It-beslutsfattare uppger att yttre påtryckningar, resursbegränsningar och ökande regelkrav hindrar dem från att bidra mer direkt till organisationens tillväxt och konkurrenskraft.

Många uttrycker en önskan om att komma närmare verksamheten och

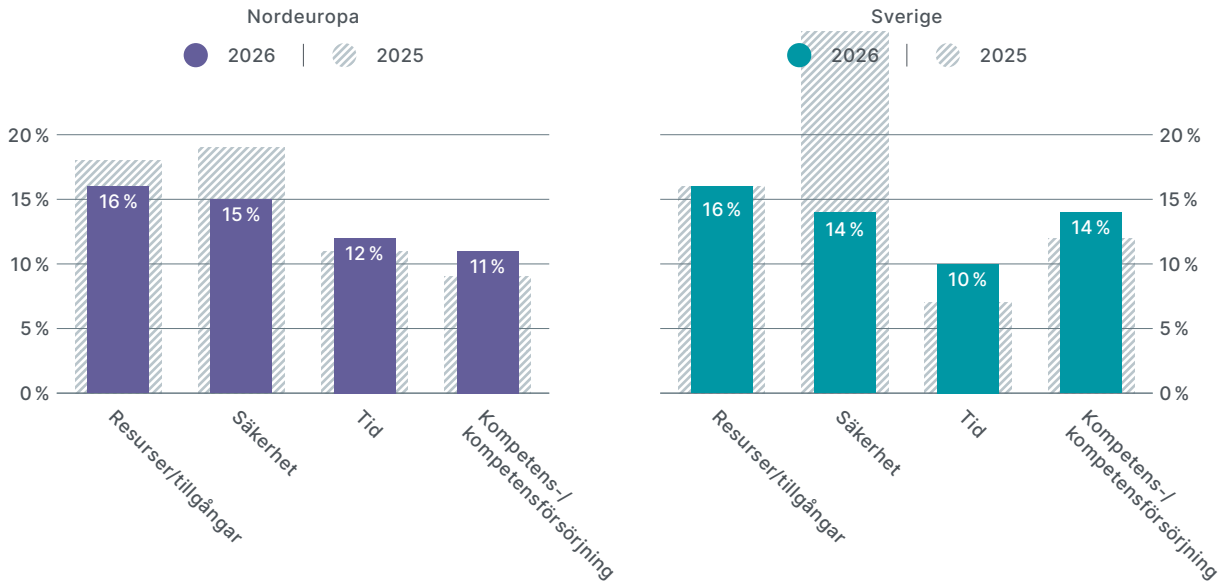
bli mer proaktiva i strategiarbetet. De lyfter fram behovet av att arbeta med mätbara initiativ som driver effektivitet. De har också en ambition att arbeta mer med innovation och automatisering. På så sätt skulle den manuella arbetsbördan minska, kompetensbristen bli mer lätthanterlig och tid för mer strategiska aktiviteter frigöras.

Det finns också en stark önskan om att skala upp AI-initiativ bortom pilotprojekt för att skapa konkret värde. It-beslutsfattare vill också investera mer tid i sitt ledarskap. Det kan handla om att ange riktning, göra avvägningar och styra prioriteringar. Sammanfattningsvis vill it-beslutsfattare se ett skifte från att lösa akuta situationer till ett mer proaktivt och framåtlatut arbetsätt.

Sverige i fokus

→ Svenska it-beslutsfattare önskar i högre grad lägga fokus på verksamhetsutveckling och digital transformation. Målet är att generera mätbara värden genom innovation, automatisering och AI, för att därmed driva tillväxt och effektivitet.

Vilken är er it-organisations största utmaning?



Den växande belastningen bakom it-avdelningarnas dagliga arbete

Sverige i fokus

→ Förra året stod säkerhet ut som den största utmaningen för svenska it-beslutsfattare. I år hamnar resurser och tillgångar i topp, med säkerhet och kompetens på delad andraplats. Tid och kompetensbrist är utmaningar som ökat från föregående år, något som riskerar att hämma organisationers utveckling och tillväxt.

Resurser och tillgångar framhålls som den största utmaningen för it-organisationer i Nordeuropa. It-beslutsfattare beskriver en miljö där kapaciteten är hårt ansträngd och där grundläggande delar av it-leveransen kräver mer uppmärksamhet än organisationen kan avsätta. Denna brist på tillgängliga resurser bromsar utvecklingen och tvingar fram svåra avvägningar långt innan det strategiska arbetet ens har påbörjats.

Säkerhet kommer tätt efter och kvarstår som en betydande påfrestning. Även om dess inflytande minskar med tiden fortsätter säkerhet att påverka budget, styrning och verksamhet. (Läs mer om it-utgifter på sidan 30.) Regleringskrav, efterlevnadsarbete och ihållande cyberhot kräver mycket fokus. (Läs mer om säkerhetsmognad och strukturella svagheter i nästa kapitel.)

Tidsbrist förstärker pressen. Obligatoriskt arbete lämnar lite utrymme för långsiktig planering eller proaktiv

utveckling. It-beslutsfattare vittnar om en ständig kamp för att avsätta tid för transformation mitt i operativa krav. Kompetensbristen, särskilt när det gäller avancerade befattningar, bidrar till utmaningen, men är ändå av underordnad betydelse jämfört med den mer generella bristen på kapacitet och tid.

Stigande kostnader spär på osäkerheten. Kostnaderna för hårdvara, molntjänster och AI-relaterad infrastruktur blir allt mer oförutsägbara, vilket försvårar planeringen och minskar flexibiliteten i investeringsbesluten.

En balansakt mellan acceleration och ansvar

När uppdraget växer i snabb takt ställs höga krav på både struktur och flexibilitet. För Läkemedelsverkets CIO Pelle Persson handlar vardagen om att balansera verksamhetsförståelse med strategiskt tänkande samtidigt som nya krav på säkerhet, AI och beredskap förändrar förutsättningarna.

Läkemedelsverket är en statlig myndighet som bland annat ansvarar för godkännande av läkemedel samt tillsyn av läkemedel och medicinteknik. Mycket av arbetet inom myndigheten styrs av EU-lagstiftning vilket påverkar it-miljön i hög utsträckning. Med ett decennium som CIO på Läkemedelsverket har Pelle Persson varit med om en omfattande förändringsresa där it-verksamheten byggts upp från grunden, samtidigt som uppdraget vuxit i takt med nya regelverk och ökade krav från omvärlden.

– Min roll handlar om att möta hela verksamhetens behov och



"Digitalisering och utveckling kommer aldrig att gå så långsamt som nu. Tempot ökar hela tiden och med det accelererar behoven."

Pelle Persson, CIO, Läkemedelsverket.

skapa it- och verksamhetsstöd som möjliggör utveckling, säger Pelle Persson.

För att fatta rätt beslut i rollen som CIO krävs balans mellan operativ närhet och långsiktig riktning.

– Man behöver stå på två ben, där det ena är verksamhetsförståelse – att vara nära verksamheten och verkligen förstå behoven. Det andra benet handlar om strategiska perspektiv och navigation i ett föränderligt landskap: Att kunna se bortom dagens behov och fundera på hur både teknik och arbetssätt kan utvecklas för att möta framtiden.

Just nu präglas arbetet av expansion. Nya regeringsuppdrag, ökade beredskapskrav och förändrad lagstiftning driver på behovet av att skala organisationen.

– Vi behöver bygga kompetens, resurser och arbetssätt som gör att vi kan skala på ett hållbart sätt.

Trots den omtalade kompetensbristen inom it-branschen upplever Pelle Persson inte rekrytering som ett avgörande hinder. Att verksamhetens behov ständigt överskrider kapaciteten är däremot en återkommande utmaning.

– Digitalisering och utveckling kommer aldrig att gå så långsamt som nu. Tempot ökar hela tiden och med det accelererar behoven. Samtidigt verkar vi i en myndighetsvärld som är relativt trög med starkt reglerade processer, budgetar

och omfattande krav. Den största utmaningen är att bli tillräckligt snabbriktig och flexibel för att möta utvecklingen.

Framåt ligger Läkemedelsverkets fokus bland annat på AI-satsningar.

– AI ger direkt verksamhetsnytta anpassade efter specifika behov. Parallellt har digital suveränitet blivit en allt viktigare fråga utifrån omvärldsläget, så vi har byggt egen kapacitet både vad gäller infrastruktur och utveckling. Myndigheten har levererat flera egna AI-lösningar, exempelvis en intern språkmodell.

Det alltmer ansträngda säkerhetsläget påverkar vardagen för Läkemedelsverkets it-verksamhet i hög grad. Säkerhet är dock inte bara en it-fråga, utan genomsyrar hela myndighetens arbete.

– Det märks i princip i allt vi gör. Dels genom ny lagstiftning, som NIS2, dels genom en allmänt ökad aktivitet från hotaktörer. Det handlar mycket om beredskap, kontinuitet och informationsklassning – att förstå vilken information som behöver vilket skydd och bygga strukturer utifrån det.

Men säkerhetskraven får inte leda till att man gör avkall på innovation och den digitala transformationen.

– Säkerhetskraven gör ofta lösningar mer omfattande och kostsamma men i grunden handlar det om att avgöra vilken information som behöver skydd. Gör man det arbetet ordentligt finns potential att skapa utrymme för innovation. ●

Redo för nuet, rustad för morgondagen

Säkerhetsmognad är en fråga om det dagliga arbetet, inte policyer. Det här kapitlet undersöker hur organisationer hanterar säkerhet i vardagen och tittar på mognadsgrad, utmaningar och incidenter. Det behandlar hur it-organisationer anpassar sig till ett föränderligt hotlandskap och tar upp hur förberedda de egentligen är på att hantera det oväntade.

Nr. 1

största
säkerhetsutmaningen: ett
fragmenterat it-landskap.

73%

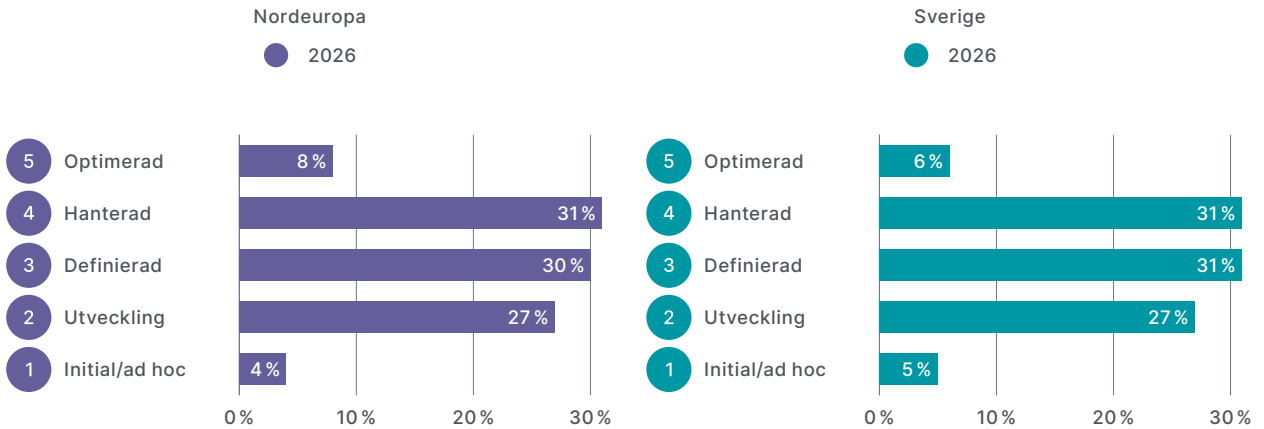
har investerat i ökad
medarbetarutbildning och
säkerhetsmedvetenhet.

76%

övar inte sina
beredskapsplaner
regelbundet.



Hur bedömer du din organisations säkerhetsmognad?



Högre mognadsgrad synliggör fler risker

Organisationer i Nordeuropa bedömer att de kommit en bit på vägen gällande säkerhetsmognad. De flesta upplever sin mognad som definierad eller hanterad. Detta visar att säkerhetsarbetet till stor del sker strukturerat. Det gör dock inte hoten mer lätthanterliga, bara enklare att upptäcka. Allt eftersom organisationerna utvecklas identifierar de fler strukturella risker inklusive legacy system, fragmenterade miljöer och kulturella klyftor. Dessa risker är ofta mindre uppenbara på lägre mognadsnivåer, där synligheten är mer begränsad. (Läs mer på sidorna 12 och 15.)

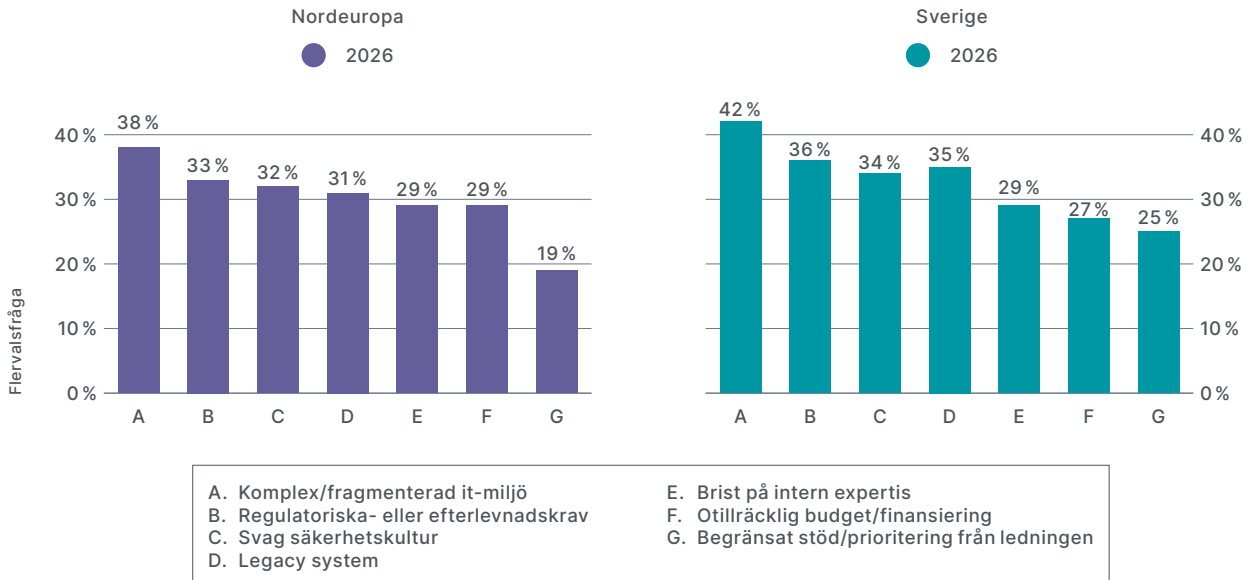
Högre mognad går hand i hand med ett starkare säkerhetsbeteende. Mer mogna organisationer rapporterar fler insatser i form av personalutbildning, internt samarbete och tekniska kontroller. De vidtar fler åtgärder för att anpassa sig till den föränderliga hotbilden samt tenderar att arbeta på ett mer kontinuerligt och systematiskt

sätt. Arbetsbördan minskar inte i takt med att mognaden ökar, istället blir det tydligare var insatser behövs. Rapporteringen av cyberattacker förstärker detta mönster. Organisationer med högre mognad upptäcker fler intrångsförsök innan de blir incidenter, eftersom de har bättre övervakning och bredare kunskap om läget. Organisationer med lägre mognad upptäcker färre attackförsök, vilket gör det svårare att förstå den reella exponeringen. Mognad stärker beredskap och reaktionsförmåga, men ger inte organisationer immunitet. (Detta diskuteras vidare på sidan 13.)

Sverige i fokus

→ Enligt Myndigheten för civilt försvar (MCF) uppvisar många svenska offentliga organisationer brister i cybersäkerhetsarbetet, där flertalet inte ens når upp till grundnivå 1 på en fyragradig skala (Cybersäkerhetskollen, 2025). När it-beslutsfattarna själva får skatta sin säkerhetsmognad hamnar den betydligt högre. Högst säkerhetsmognad rapporteras inom privat sektor, särskilt i stora organisationer. Mogna organisationer har ofta en mer robust säkerhetskultur och färre utmaningar med budget och intern expertis. Närmare 7 av 10 (69 procent) som övar regelbundet på sina incidenthanteringsplaner anser sig ligga på de två högsta mognadsnivåerna.

Vilka är de främsta utmaningarna i er organisations säkerhetsarbete?



Därför är säkerhetsarbetet svårare än det borde vara

Sverige i fokus

→ I Sverige anses utmaningarna med legacy system allt mer akuta, framför allt inom privat sektor. För att dessa ska erkännas som en utmaning krävs det en viss grad av säkerhetsmognad. Mindre mogna aktörer kämpar med vad exempelvis NIS2/ Cybersäkerhetslagen innebär och avvaktar därför tydligare föreskrifter. Dessa organisationer kämpar också med en svag säkerhetskultur, bristande intern kompetens och otillräckligt stöd från ledningen.

Säkerhetsarbetet präglas i allt högre grad av strukturella hinder snarare än enskilda incidenter. Den största utmaningen är komplexiteten i de tekniska miljöerna. Fragmenterade system leder till isolerade säkerhetskontroller och en ofullständig överblick, vilket gör det svårt att genomföra moderna försvarsstrategier. Detta tvingar it-beslutsfattare att prioritera konsolidering och plattformsanvändning framför att införa nya verktyg.

Regulatoriska påtryckningar är en utlösande katalysator. Många organisationer agerar på grund av obligatoriska krav snarare än strategiska avsikter. När strikta tolkningar av regelverk prioriteras före ett strategiskt säkerhetsarbete riskerar det att öka kostnader och minska långsiktig motståndskraft.

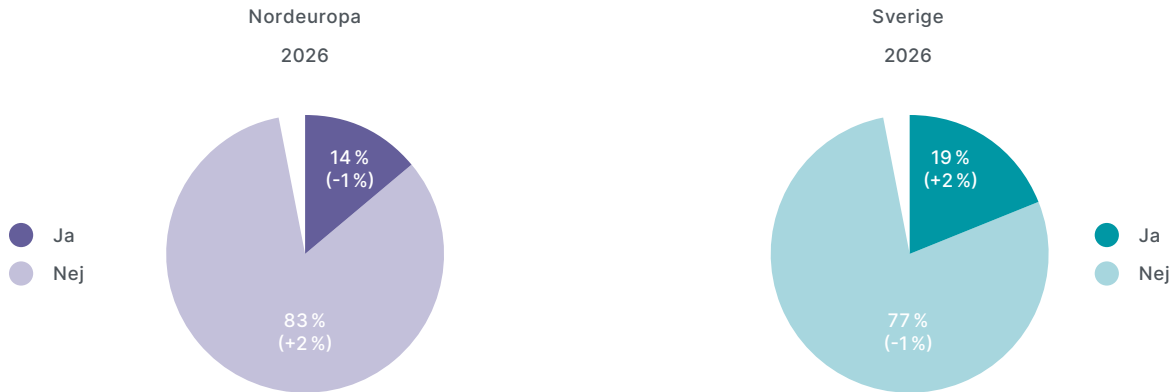
Säkerhetskulturen fortsätter att vara en grundläggande utmaning, särskilt för organisationer med lägre mognadsnivåer. Utan konsekvent beteende,

utbildning och engagemang hos hela personalstyrkan kan tekniska investeringar inte leverera sitt fulla värde.

Legacy system tillför ytterligare en riskfaktor då de ofta är svåra eller kostsamma att säkra. Organisationer med högre säkerhetsmognad är ofta mer medvetna om riskerna medan många andra underskattar exponeringen i äldre arkitekturer. Även här finns en klyfta mellan upplevd beredskap och faktisk sårbarhet.

Utvecklingen hämmas ytterligare av bristen på intern säkerhetsexpertis. Även om externa partners kan stödja säkerhetsarbetet måste ägarskapet förbli internt för att undvika att ansvaret blir otydligt. I takt med AI-utvecklingen ökar både hot och operativ komplexitet, vilket gör luckor i styrning och identitetskontroll mer synliga. Organisationer inom offentlig sektor kämpar mer med finansiering, medan aktörer inom privat sektor står inför teknisk fragmentering.

Har ni upplevt några cyberattacker under de senaste 12 månaderna som påverkat er organisations förmåga att fungera normalt?



Siffror inom parentes visar förändringen jämfört med förra året (procentenheter).

Incidenter driver aktivitet men skapar inte immunitet

En minoritet av organisationerna i Nordeuropa rapporterar att de under det senaste åren har drabbats av en cyberattack med konsekvenser för verksamheten. Dessa incidenter fungerar som en katalysator för ökad aktivitet snarare än ett tecken på bristfällig säkerhet. Organisationer som har utsatts för attacker rapporterar ofta fler utmaningar som fragmentering, påtryckningar från lagstiftning, svag säkerhetskultur och legacy system. En attack synliggör ofta problem som redan fanns.

Ökad aktivitet efter en incident leder dock inte automatiskt till varaktig mognad. Många organisationer uppdaterar planer, reviderar processer eller övar på åtgärder efter en attack, men förbättringarna är ofta kortsiktiga och reaktiva. Verkligen motståndskraft kräver ihållande, proaktivt arbete.

Säkerhetsmognad garanterar inte färre allvarliga attacker. Organisationer med hög säkerhetsmognad rapporterar fortfarande incidenter, troligen på grund av bättre detektionsförmåga och bredare attackytor. Mindre mogna

organisationer kan ha upptäckt färre händelser. Siffrorna över de som svarat att de inte utsatts för några attacker bör därför avläsas med försiktighet. Stark detektering och övervakning är avgörande för att förstå den verkliga exponeringen.

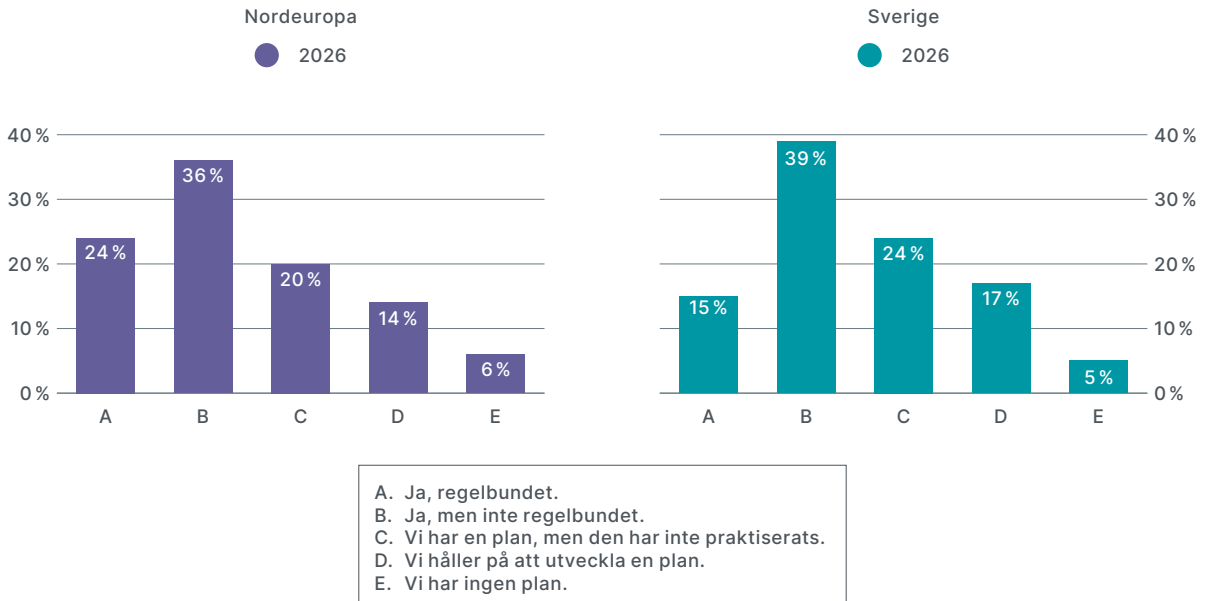
Sannolikheten att rapportera en attack påverkas också av vilken sektor ens organisation tillhör och ens storlek. Sverige sticker ut i jämförelse med övriga länder i undersökningen med högre rapporteringsgrad vilket kan indikera bättre detektionsförmåga eller striktare rapporteringsrutiner.

Cyberattacker belyser ofta underliggande svagheter, särskilt i fragmenterade eller äldre miljöer. Utan ett starkt internt ägarskap för säkerhet och ett uttalat fokus på kontinuitet riskerar organisationer att bli beroende av externa partners vid kritiska händelser. Beredskap måste omfatta AI-drivna attackscenarier, eftersom angripare i allt högre grad använder automatisering och identitetsfokuserade tekniker.

Sverige i fokus

→ En högre andel svenska respondenter (19 procent) har upplevt cyberattacker med påverkan på verksamheten jämfört med Nordeuropa i stort (14 procent). Offentliga organisationer i Sverige som drabbats uppvisar specifika utmaningar som regleringsrelaterade faktorer, svag säkerhetskultur och begränsad support/prioriteringar från ledningen. En engagerad ledning är avgörande.

Har ni övat på er organisations plan för att hantera oförutsedda händelser?



De flesta planer är oprövade när det verkligen gäller

Sverige i fokus

→ En lägre andel svenska organisationer övar regelbundet på sina planer än snittet för Nordeuropa, 15 mot 24 procent. Det kan förklaras med en hög andel kommunala it-beslutsfattare bland svenska respondenter. Endast 7 procent av Sveriges kommuner övar regelbundet. Svensk offentlig sektor övar generellt mindre än offentlig sektor i andra länder. Privat sektor övar betydligt oftare. Säkerhetsarbetet i Sverige har länge kretsats kring förebyggande åtgärder men ser nu ut att vara på väg mot ett mer operativt fokus. Här har införandet av mer strukturerade rutiner spelat stor roll.

Hur mycket organisationer övar på sina beredskapsplaner skiljer sig i Nordeuropa. Endast en fjärdedel övar regelbundet på sina incidenthanteringsplaner. Det innebär att många förlitar sig på planer som inte har testats under realistiska förhållanden eller endast vid ett fåtal tillfällen. En plan dokumenterar ansvar och åtgärder, men behöver återkommande övning för att kunna stödja snabba beslut i pressade situationer.

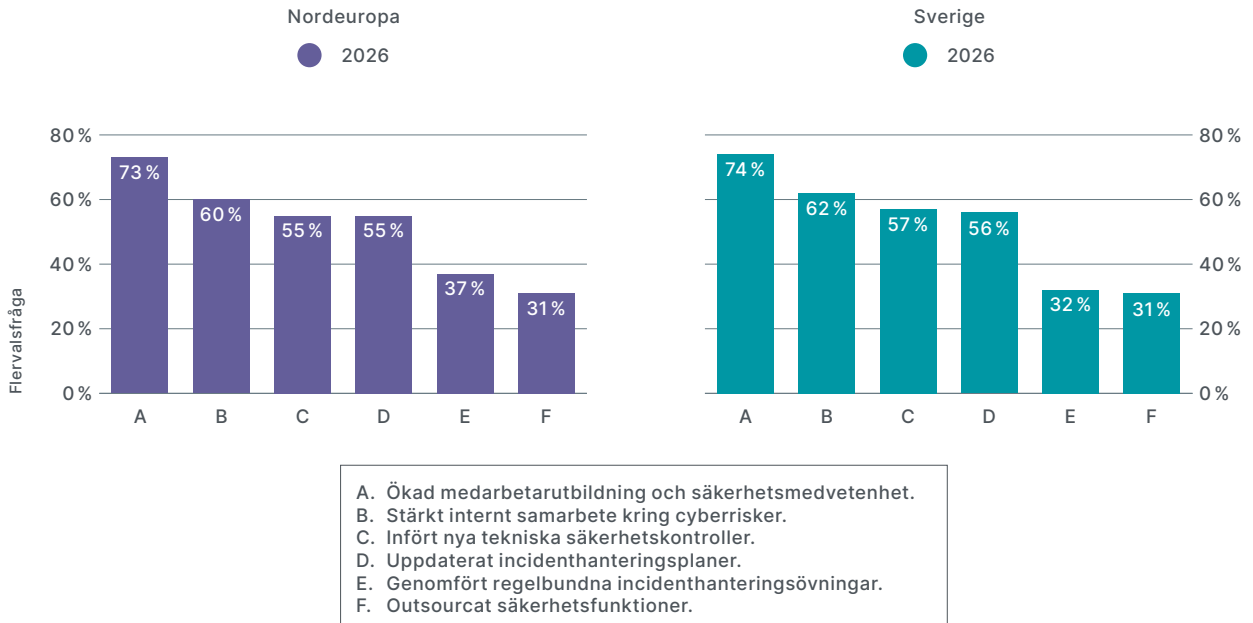
Idag tenderar fokus i övnings-scenarier att ligga på externa attacker. Exempel på dessa är ransomware, intrång i infrastrukturen eller andra yttre hot. Insider-relaterade händelser ingår sällan, trots att dessa situationer är svårare att upptäcka och kräver snabba bedömningar. Det leder till brister i beredskapen.

Verksamhetens kontinuitet måste återspeglas i effektiv övning. Tekniska åtgärder är bara en del av hanteringen av en oförutsedd händelse. Övningar

måste innefatta ledningens prioriteringar av kritiska tjänster, kommunikationsvägar i organisationen och beslut om återställning när flera funktioner drabbas samtidigt. Externa partners kan stötta utförandet, men det interna ledarskapet måste styra.

Det finns ett starkt samband mellan säkerhetsmognad och regelbunden övning. Organisationer med hög säkerhetsmognad övar betydligt oftare än mindre mogna organisationer som sällan kommit längre än nedskrivna planer. Regelbunda övningar bör med andra ord inte underskattas utan ses som en avgörande ingrediens för verksamhetens beredskap.

Hur har er organisation anpassat sig till den ändrade hotbilden under de senaste 12 månaderna?



Säkerhetsarbetet anpassas efter omvärldsläget

De flesta organisationer vidtar gradvisa åtgärder för att anpassa sig till den föränderliga hotbilden. Det handlar främst om att utbilda personal, införa nya tekniska kontroller, uppdatera incidenthanteringsplaner och stärka samarbetet mellan it, verksamhet och ledning. Dessa är alla nödvändiga åtgärder, men de omformar inte säkerhetsstrategierna.

Utbildning är den vanligast förekommande åtgärden. Det stärker både säkerhetskulturen och ökar riskmedvetenheten. Det interna samarbetet har ökat från tidigare år vilket tyder på ett större engagemang från alla delar av organisationen, inklusive ledningen.

Organisationer med högre säkerhetsmognad har i större utsträckning genomfört fler åtgärder.

AI ökar effektiviteten och kapaciteten dramatiskt, med både positiva och negativa följder. Det påskyndar behovet av anpassning, men inte genom helt nya hotkategorier.

AI sänker tröskeln för angripare genom mer precis inriktning. Denna utveckling gör befintliga attackmetoder mer effektiva. Organisationers användning av AI kan öka den framtida exponeringen, men dess praktiska inverkan på anpassningen är hittills blygsam.

Slutsatsen är att anpassning sker, fast ojämnt. Mogna organisationer gör större framsteg, medan små och mindre mogna organisationer tar sporadiska steg utan en övergripande plan.

Sverige i fokus

→ I Sverige har mjuka investeringar, såsom administrativa och organisatoriska åtgärder, ökat som ett proaktivt svar på den föränderliga hotbilden. Svenska organisationer övar mindre regelbundet på sina incidenthanteringsplaner än organisationer i övriga Nordeuropa.

På Pite Energi ligger det yttersta säkerhetsansvaret hos ledningen

Som samhällskritisk aktör är energisektorn ett attraktivt mål för cyberangrepp. För Pite Energi är beredskap och säkerhetskultur en nödvändighet för att kunna upprätthålla samhällsviktiga funktioner.

Jörgen Andersson Strand är vd på energibolaget Pite Energi – en verksamhet som sysslar med allt från elhandel och elnät till fjärrvärme och bredband. Med en bakgrund som officer är han väl medveten om den roll energiförsörjning spelar i samhällets motståndskraft och att energisektorn är ett attraktivt mål för cyberangrepp.

– Attacker sker hela tiden, mot alla, kanske särskilt mot energibranschen som ständigt är ett prioriterat mål. Energiförsörjning, tillsammans med logistik och kommunikation, har alltid varit centralt i militära planer.

För Pite Energi handlar det inte bara om affär och lönsamhet utan om att upprätthålla grundläggande samhällsfunktioner som energi, värme och digital infrastruktur. Med det följer ett ansvar för säkerhet.

– Vi har bedrivit seriöst säkerhetsarbete och arbetat strukturerat och systematiskt med säkerhetsfrågor länge. På koncernnivå har vi en kris- och resursplan och varje verksamhetsområde har egna kontinuitets- och krisplaner.

Nyckeln för att lyckas med säkerhetsarbetet är enligt Jörgen Andersson Strand att regelbundet öva.

– Förberedelse och beredskap är A och O. När vi övar ett scenario hittar vi alltid saker som behöver förbättras. Planerna är levande dokument som hela tiden utvecklas.

En annan avgörande faktor är att ledningen driver frågorna.

– Det yttersta ansvaret ligger hos ledningsgruppen. Vill man att säkerhet ska vara prioriterat i verksamheten måste ledningen visa vägen. Där skapas säkerhetskulturen som sedan genomsyrar hela organisationen.

Med ansvar för säkerhet följer också utmaningar.

– Den största utmaningen just nu är säkerhetsläget i omvärlden. Dessutom är hela branschen på en stor digitaliseringsresa, med AI som kommer in i systemen och elnät som behöver moderniseras. Digitaliseringen gör oss effektivare, men riskerna ökar när system exponeras mot internet. Dessutom kommer många olika lagkrav som ska uppfyllas.

Jörgen Andersson Strand ser dock de regulatoriska kraven som stöd till verksamheten.

– Det är tydliga lagkrav som inte går att bortse från, men som gör det lättare att motivera åtgärder gentemot styrelse och ägare.

Det är inte bara lagkrav som Pite Energi behöver förhålla sig till. Som offentligt bolag har de högre krav på transparens och insyn jämfört med privat sektor.

– Även om säkerhetskraven också ökar på privata aktörer ställs högre krav på oss, både från samhället och ägarna, då det utåt sett är tydligare vad vi gör och inte.

Samtidigt ser Jörgen Andersson Strand offentligt ägarskap som en möjliggörare för handlingsutrymme inom säkerhetsinvesteringar.



"Förberedelse och beredskap är A och O. När vi övar ett scenario hittar vi alltid saker som behöver förbättras."

Jörgen Andersson Strand, vd, Pite Energi.

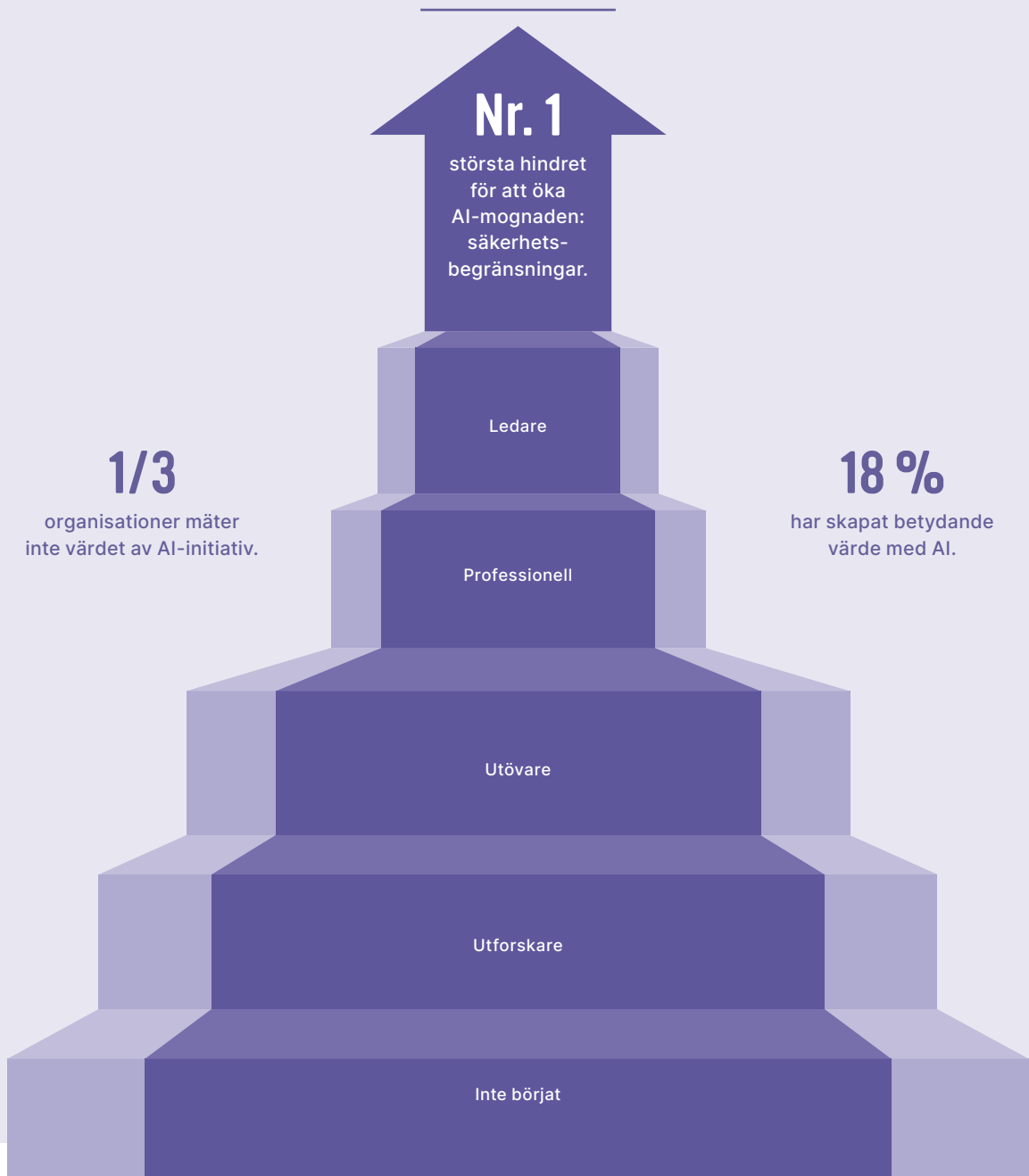
– Det finns en större förståelse hos kommunala och statliga ägare för att säkerhet är kostsamt. Lönsamhetskraven är ofta inte lika hårda, vilket gör det lättare att prioritera resurser till säkerhetsåtgärder.

Och säkerhet kommer att vara en fortsatt prioritet för Pite Energi. Jörgen Andersson Strand återkommer till vikten av förberedelse:

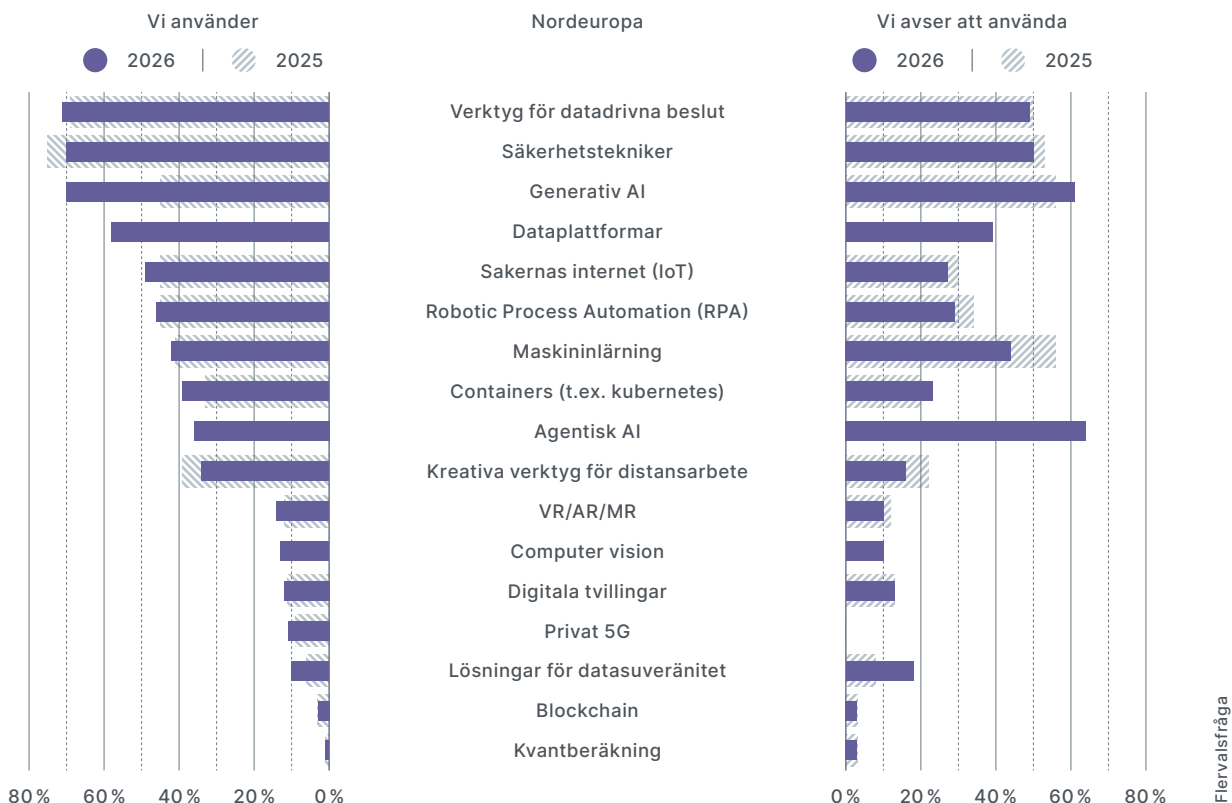
– Vi identifierar risker och försöker skydda oss så långt det går, men är också förberedda på att något oförutsägbart ändå kan ske. Backup, återställning och möjligheten att bedriva kritisk verksamhet manuellt är avgörande. ●

Frigöra värdet: från utforskare till utövare

Ambitionen med AI sträcker sig bortom enbart pilotprojekt.
Det här kapitlet belyser hur organisationer överkommer hinder,
skapar betydande värde och bedömer effekterna av sina AI-initiativ.
Det ger insikter kring vad som skiljer utforskarna från utövarna.



Vi använder följande tekniker...



Från assistenter till agenter: nästa fas i AI-användningen

Sverige i fokus

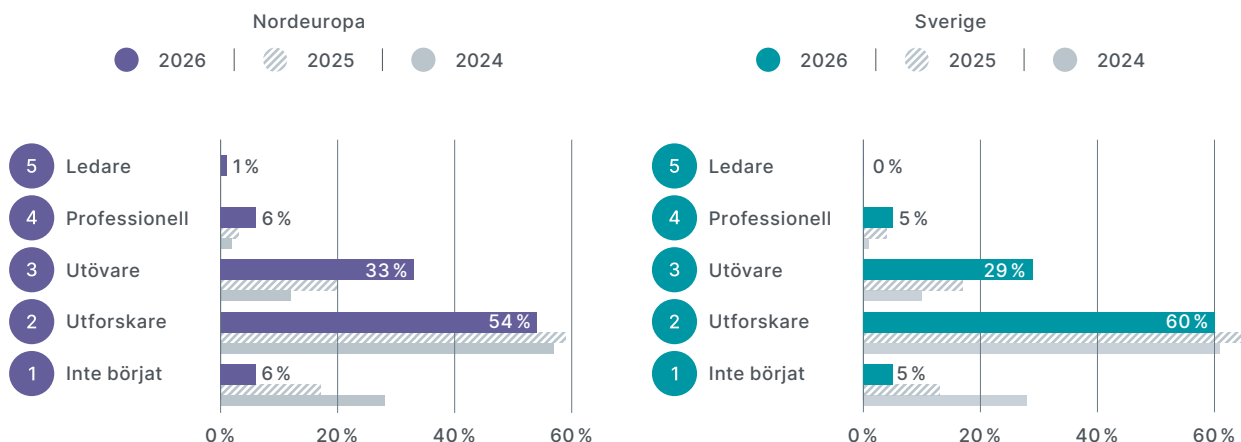
→ Sverige använder maskininläring (ML) i mindre utsträckning än övriga Nordeuropa, 33 jämfört med 42 procent. Svenska organisationer använder även verktyg för datadrivna beslut i mindre utsträckning, 62 jämfört med dryga 70 procent. Samtidigt visar Sverige en större vilja än övriga länder i Nordeuropa att öka sin användning de kommande tre åren. Utöver verktyg för datadrivna beslut önskar svenska organisationer även öka sin användning av agentisk AI.

Teknikanvändningen i Nordeuropa går allt mer mot AI. Generativ AI uppvisar den starkaste tillväxten och används nu i stor utsträckning i produktion. Organisationer planerar samtidigt för en betydande utbyggnad av agentisk AI under de kommande åren. AI-mogna organisationer som redan använder mer avancerade AI-verktyg avser att skala upp dem ytterligare. Maskininläring förblir en viktig värdeskapare, särskilt bland organisationer med hög mognadsgrad som har integrerat den i sin verksamhet. Tekniker såsom VR, digitala tvillingar, blockchain och computer vision som tidigare omgavs av stora förhoppningar på marknaden har inte fått det genomslag som förväntades.

Istället fokuserar organisationer på verktyg som stöder produktivitet och automatisering.

Detta skifte kan förklaras av den breda användningen av AI. Innehållsskapande, kodningsstöd, interna chattrobotar samt applikationer för it- och cybersäkerhet är nu vanliga. Mer avancerade användare integrerar AI i verksamheten, prognoser och automatisering, där vinsterna är större och lättare att kvantifiera. Maskininläring och agentisk AI är de tekniker som mest förknippas med stort värdeskapande, även om den förväntade tillväxten är störst inom agentisk AI.

Hur bedömer du din organisations AI-mognad?



Svårt att gå från experiment till genomförande

AI-mognaden i Nordeuropa ökar. Andelen organisationer som befinner sig i stadiet ”inte börjat” har minskat avsevärt, och många avancerar genom mognadsnivåerna i en stadig takt. Övergången från utforskare till utövare är konsekvent och pilotprojekt lämnar utrymme för mer standardiserade AI-funktioner och tydligare målsättningar.

Utvecklingen saktar in på utövarnivån. Det är nämligen då som organisationer börjar att operationalisera AI och integrera tekniken i sina processer. Skalning kräver dock styrning, övervakning och uppdaterade driftsmodeller – kapaciteter som tar tid att bygga upp. Den långsamma ökningen av organisationer som når nivån professionell visar på svårigheter att gå från pilotprojekt till att på riktigt transformera verksamheten.

Finland har en märkbart högre koncentration av mogna organisationer än övriga länder i Nordeuropa,

med 62 procent på nivåerna 3 till 5 jämfört med genomsnittet på 40 procent. Organisationer på dessa höga mognadsnivåer uppger ett större värdeskapande. Mindre mogna organisationer fortsätter att experimentera utan att systematiskt utvärdera sina resultat.

Kompetensutveckling är fortfarande den utmaning som nämns oftast, särskilt bland organisationer som redan har skapat ett visst värde och vill ta nästa steg. Osäkerhet kring regelverk och säkerhetsbegränsningar hämmar också utvecklingen, särskilt i offentlig sektor där frågor om regelefterlevnad och suveränitet är väsentliga. Att göra framsteg bortom utövarnivån kräver tid, tydlighet och en stark organisatorisk grund.

Sverige i fokus

→ AI-mognaden ökar långsammare i Sverige än i övriga länder. Visserligen har utövarna (nivå 3) blivit fler och nybörjarna (nivå 1) färre, men många har stannat som utforskare (nivå 2). Dessutom är förflyttningen till professionell (nivå 4) begränsad. Den lägre mognadsgraden i Sverige kan troligen förklaras av osäkerhet kring regelverk och brister i ledarskap. Båda dessa hinder spelar en stor roll för organisationer som har svårt för att ta sig vidare från nivå 2 till nivå 3. I takt med ökad AI-användning i Sverige förväntas även kompetensbristen bli en allt större utmaning.

Min organisation har skapat betydande värde med AI.



Värdeskapandet med AI ökar långsamt trots snabb mognad

Sverige i fokus

→ Trots lägre AI-mognad i Sverige jämfört med andra länder i undersökningen rapporterar 18 procent av organisationerna högt värdeskapande med AI, vilket motsvarar genomsnittet för Nordeuropa. Det tyder på framgångar för svenska organisationers AI-satsningar, även om den allmänna mognadsgraden inte har utvecklats lika snabbt. Organisationer som uppnår högre värden med AI använder ett brett spektrum av tekniker, däribland maskin-inlärning och agentisk AI.

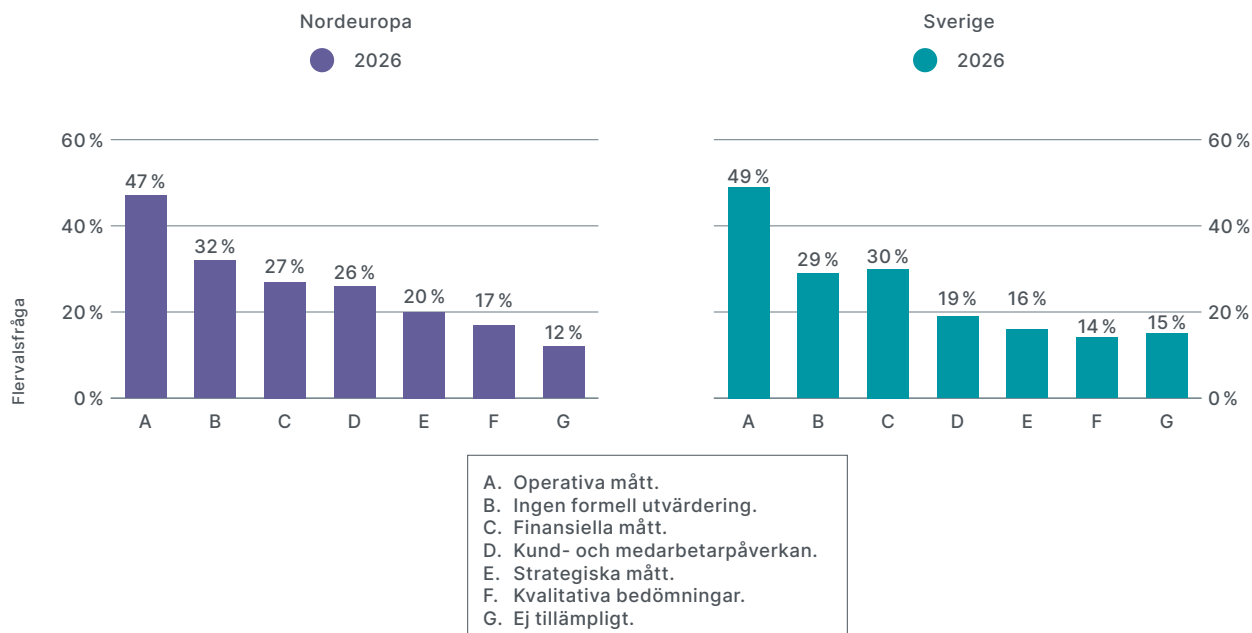
Organisationer i Nordeuropa visar på framsteg inom värdeskapande med AI men det går långsammare än mognadsutvecklingen. Även om fler organisationer har nått nivån ”utövare” eller högre har andelen som skapat betydande värde med AI endast ökat marginellt. Trots tydlig struktur och uttalade ambitioner verkar den bredare verksamhetsnyttan inte ha uppnåtts.

Organisationer på utövernivå rapporterar trots allt mer värde än utforskare, men befinner sig fortfarande på en plåtå där pilotprojekt dominerar. Meningsfullt värde uppstår senare under resan. Organisationer på nivåerna ”professionell” och ”ledare” rapporterar det högsta värdet med en betydande marginal. Drivkrafter bakom mätbara resultat är affärs-transformation, integration och skalbara piloter.

Mindre mogna organisationer har svårt att utvärdera värdet över huvud

taget. Avgränsade projekt och piloter gör det svårt att mäta produktivitetsvinster, tidsbesparingar eller operativa förbättringar. Mogna organisationer tenderar att lägga fokus på operativa nyckeltal snarare än finansiella resultat. På så sätt blir det enklare att mäta värde och införa AI i verksamhetens dagliga processer. (Läs mer om AI-användning på sidan 18.)

Hur utvärderar er organisation affärsvärdet av sina AI-initiativ?



Många organisationer inför AI utan en mätbar strategi

Organisationer i Nordeuropa utvärderar främst AI utifrån operativa mått. Det innebär att titta på produktivitetsvinster, processautomatisering och tidsbesparingar för att bedöma om initiativen skapar värde. Detta förekommer särskilt i mogna organisationer, där AI är integrerat i den dagliga verksamheten och resultaten syns i arbetsflödena.

Samtidigt uppger ungefär en tredjedel av it-beslutsfattarna att deras organisation formellt sett inte utvärderar affärsvärdet med AI. Det gör att många inte bestämt hur resultat av projekt och verktyg ska mätas.

Klyftan är tydligast på lägre mognadsnivåer. Utforskare och tidiga användare saknar ofta strukturerade ramverk för utvärdering. Deras projekt är svåra att kvantifiera effekten av på ett strukturerat sätt. Som ett resultat har it-beslutsfattare svårt att jämföra initiativ eller argumentera för skalbara investeringar.

Organisationer med högre AI-mognad tar hänsyn till värdeaspekter redan i utformningen och valideringen av användningsfall. Mätvärden definieras tidigt, uppdateras i takt med att lösningen utvecklas och används för att justera eller avbryta initiativ.

Helhetsintrycket är splittrat. Många it-beslutsfattare har tagit AI i drift, men en betydande andel saknar fortfarande en tydlig bild av om AI gör organisationen mer effektiv. Att komma förbi detta hinder blir avgörande för att besluta vilka AI-initiativ som förtjänar att skalas upp och vilka som bör förbli experiment.

Sverige i fokus

→ AI-mogna organisationer är bättre på att mäta värdet av sin AI-användning än mindre mogna organisationer. Det visar på ett samband mellan AI-mognad och värdeskapande, där hög AI-mognad innebär att man både är bättre på att skapa värde samt mäta det. I Sverige är det marginellt färre som inte gör någon formell utvärdering alls än i övriga länder. Att en organisation mäter värde tyder på en mognare och mer strukturerad process för användningsfall, något som är centralt för att i slutändan skapa värde med AI.

AI måste driva affärsnytta – inte bara teknisk innovation

Genom tydlig styrning, fokus på affärsnytta och en stabil grund har Bastard Burgers byggt sin AI-mognad. Tekniken används idag brett i verksamheten och Johnny Bröms, Chief Digital & Technology Officer, menar att AI kommer att få en ännu större och mer betydande roll framåt.

Johnny Bröms ansvarar för it och digital utveckling på premiurgarkedjan Bastard Burgers. Med lång erfarenhet från både it- och restaurangbranschen driver han arbetet med att förena affär och teknik. I dag handlar det mycket om att leda bolagets digitala transformation med AI som en naturligt integrerad del av verksamheten.

När han tillträdde 2023 möttes han av en fragmenterad it-miljö utan tydlig riktning. Arbetet inleddes därför med att skapa struktur och en gemensam väg framåt.

– Första steget var en nulägesanalys. Därefter byggde vi en stabil grund, följt av ett mer agilt arbetssätt och närmare koppling mellan teknik och affär – med målet att digitala lösningar ska vara fullt integrerade i affärsprocesserna.

I dag används AI praktiskt inom flera delar av verksamheten. Ett område är avtalshandling där AI-baserade stöd analyserar avtal utifrån interna riktlinjer. Man har även utvecklat flera AI-agenter, bland annat en för konkurrensanalys. Ytterligare exempel finns inom it-supporten där en supportagent byggts ovanpå interna plattformar och system.

– Eftersom vi köper externa it-supporttjänster varierar kompetensnivån. Med hjälp av AI-agenten kan supporten snabbt få svar på hur våra system fungerar, hur ärenden ska lösas och vilka åtgärder som rekommenderas. Vårt nästa steg blir



"Det är lätt att fastna i tekniken, men att förstå hela livscykeln är avgörande."

Johnny Bröms, Chief Digital & Technology Officer, Bastard Burgers.

att sätta en AI-baserad lösning för gästkommunikation i produktion, som ska hantera frågor om exempelvis öppettider, produkter och allergener.

Årets CIO Analytics-rapport visar att en central utmaning med AI är att skapa affärsvärde med tekniken, något som Johnny Bröms kan relatera till. På Bastard Burgers har man därför etablerat flera råd, med fokus på affär och verksamhetsnytta, där idéer och behov fångas upp samt analyseras. Även utvärdering är en viktig del av arbetet där uppföljning sker både genom mätbara resultat och kvalitativa jämförelser.

– Det är lätt att fastna i tekniken, men att förstå hela livscykeln är avgörande. Investeringskostnader, långsiktig drift och säkerställandet av funktion även om nyckelpersoner försvinner är parametrar som bör tas i beaktning.

I takt med ökad AI-användning blir frågor om säkerhet, styrning och datakvalitet allt viktigare. För Bastard Burgers handlar arbetet främst om affärsnytta, kvalitetssäkring och kontroll.

– Datakvaliteten var en stor utmaning i början. Vi har behövt gå igenom system för system och säkerställa att data är korrekt och tillförlitlig. För oss handlar AI än så länge om att sammanställa underlag, ge rekommendationer och beslutsinriktning. I dag har vi inga processer där AI själv fattar beslut.

I nuläget bedömer Johnny Bröms Bastard Burgers AI-mognad som relativt hög, men långt ifrån fulländad.

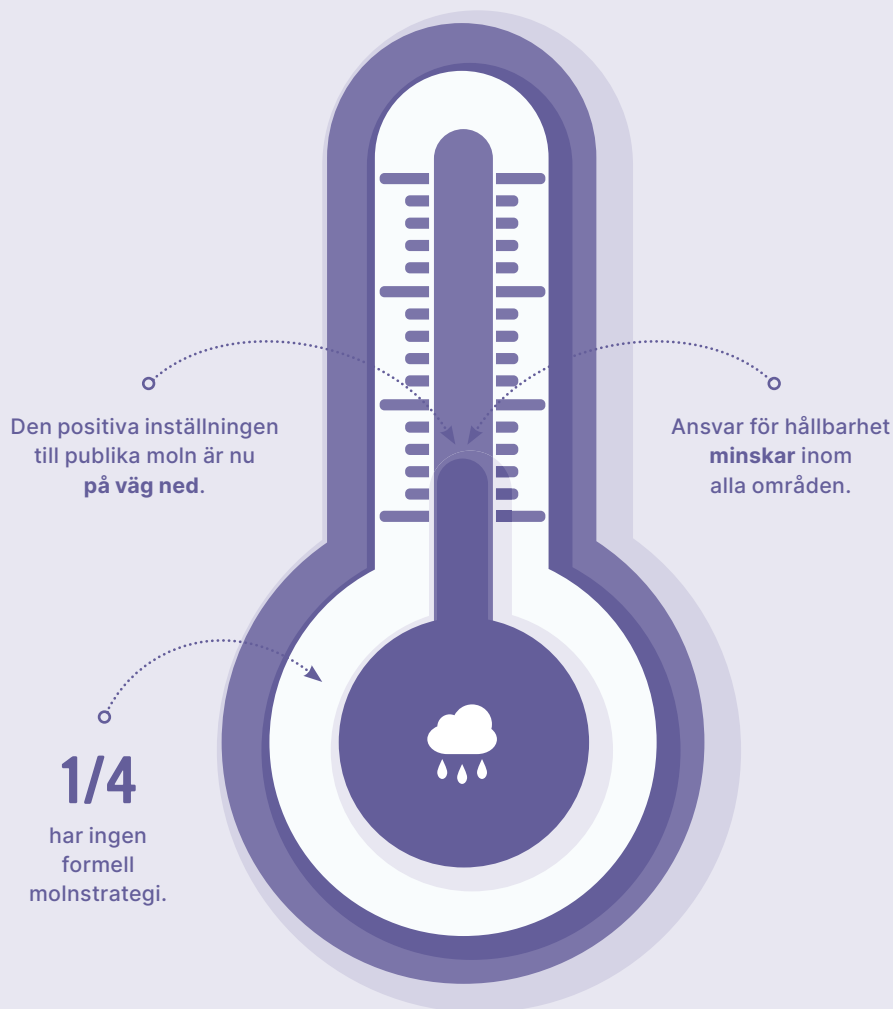
– Jag är inte helt nöjd, men vi har kommit långt. Framför allt har vi byggt en förståelse för vad vi vill använda AI till och varför. Vi arbetar strukturerat med styrning, en mognadstrappa och en tydlig verktygsstrategi.

Framåt väntas AI få en ännu större roll, inte minst i gästupplevelsen och interna effektiviseringar, med en tydlig riktning:

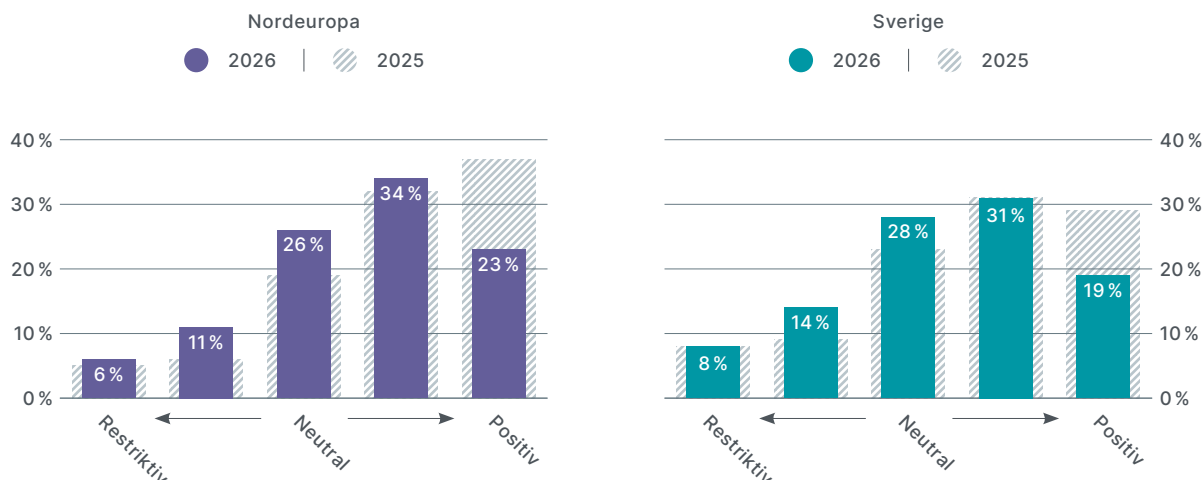
– Vårt fokus kommer fortsatt att vara detsamma – AI ska driva affärsnytta, inte bara teknisk innovation. ●

Förändrade perspektiv på moln och hållbarhet

Inställningarna till moln och hållbarhet fortsätter att förändras. Det här kapitlet visar hur organisationer ser på publika moln, definierar strategier, balanserar sina team och kopplar it-beslut till bredare hållbarhet och organisatoriskt ansvar.



Vad är er organisations nuvarande inställning till att använda publika molnlösningar?



Från optimism till neutralitet: attityderna till publika molntjänster förändras

Sverige i fokus

→ Svenska it-beslutsfattare har en fortsatt försiktig hållning till publika molntjänster. Etablerade molnstrategier saknas i högre grad inom offentlig sektor, vilket sammanfaller med en mer restriktiv inställning. Även inom privat sektor minskar andelen mycket positiva svar i år. Det tyder på en mer restriktiv syn även där. En ökad drivkraft till att använda publika molntjänster är att kunna utveckla funktioner som organisationerna inte kan utveckla internt. Detta kan bero på ökade behov av avancerade plattformar och tjänster drivet av AI, tekniska krav samt behov av flexibel kapacitet.

Efter flera år av ökad positivitet har attityderna till publika molntjänster dämpats i Nordeuropa under 2026. De flesta är fortfarande generellt positiva, men färre beskriver sin inställning som mycket positiv. I stället intar fler respondenter en neutral eller försiktigt positiv position. Förändringen speglar en växande tveksamhet snarare än minskad molnanvändning.

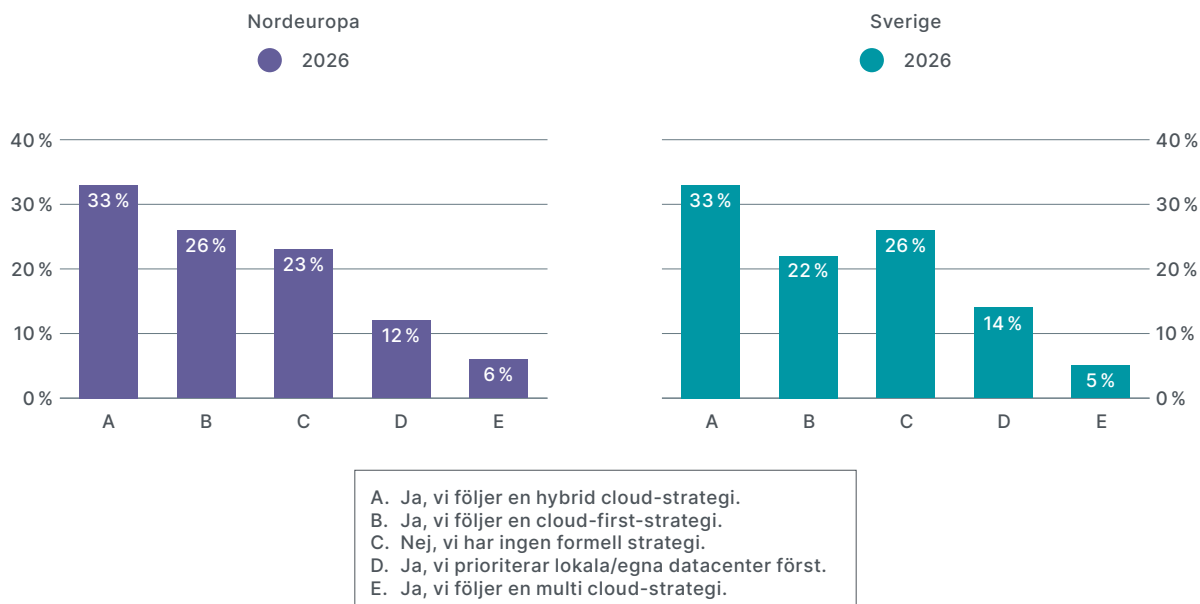
Inställningen skiljer sig mellan privat och offentlig sektor. Privat sektor visar en brantare nedgång i stark positivitet, från 45 till 26 procent, medan offentlig sektor minskar från 26 till 18 procent. Detta indikerar olika utgångspunkter och grader av förändring.

Bakom den nedåtgående trenden finns flera hinder. Säkerhetsfrågor är fortfarande det hinder som nämns oftast och fortsätter att påverka förtroendet. Suveränitet och geopolitiska överväganden har blivit allt viktigare. Många organisationer

väger nu exponering mot gränsöverskridande beroenden och strategiska konsekvenser av molnkoncentration. Rättslig osäkerhet är fortfarande ett stort hinder, även om dess relativa betydelse har minskat med tiden. Kostnaden och oförutsägbarheten för molnutgifter fortsätter också att dyka upp som praktiska problem.

Trots dessa hinder kvarstår drivkrafter för att använda publika molntjänster. Organisationer fortsätter att förlita sig på publika molntjänster för skalbarhet, hög tillgänglighet och tillgång till specialiserade tjänster som de skulle ha svårt att producera själva. Att positiviteten dämpats handlar alltså inte om ett minskat beroende av publika molntjänster utan en mer försiktig och riskmedveten inställning.

Har er organisation en definierad molnstrategi?



Strategi snarare än teknik styr tilliten till molntjänster

Införandet av molnstrategier varierar avsevärt i Nordeuropa och huruvida en organisation har eller inte har en fastställd strategi är ett tydligt mönster bland respondenterna. Endast 16 procent inom privat sektor saknar en strategi. Motsvarande andel inom offentlig sektor är 32 procent. Det återspeglar strukturella skillnader i hur beslut om molnet organiseras.

Respondenter utan en formell strategi tenderar att vara mindre positiva till publika molntjänster. De som prioriterar lokala lösningar är mest restriktiva. Däremot uttrycker organisationer med definierade molnstrategier större förtroende och ett mer medvetet förhållningssätt till att integrera publika molntjänster.

Beslut om var arbetslaster ska köras domineras av två överväganden: säkerhetskrav och total ägandekostnad. Dessa faktorer utgör kärnan i ens molnstrategi och påverkar placeringen av arbetslaster för samtliga länder

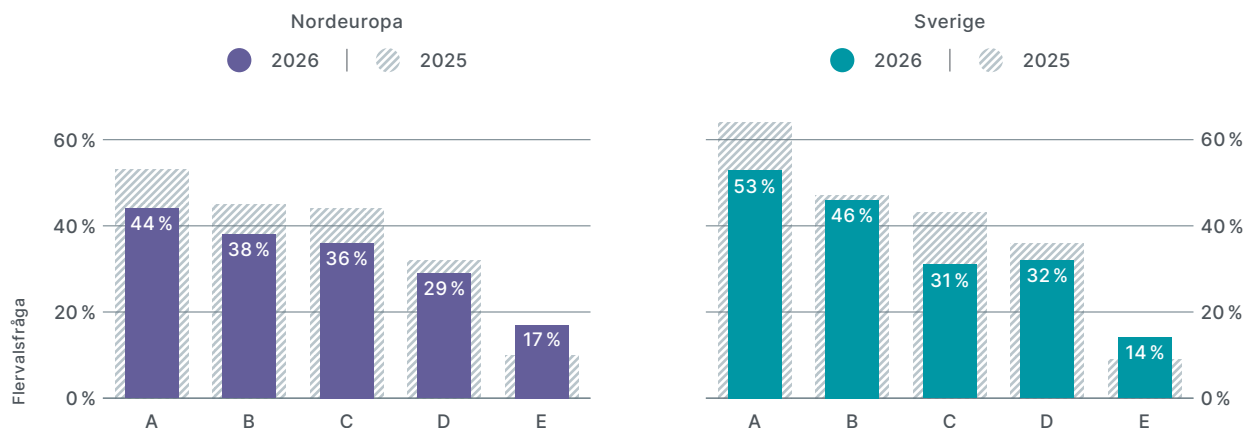
och sektorer. Även om hållbarhet ofta framhålls som en fördel med molnet har den liten betydelse för beslutsfattandet (10 procent) jämfört med säkerhet (74 procent) och kostnad (68 procent).

Trots att säkerhet är en av de viktigaste faktorerna vid placering av arbetslaster är riskbedömningar inte en avgörande faktor för de flesta (endast 17 procent). Det kan tyda på ett antagande om att molnplattformar är säkra redan från början och ett överdrivet förtroende snarare än en strukturerad utvärdering. Känsligheten för datalagring och suveränitet varierar mellan olika länder, vilket understryker att molnstrategier måste balansera operativa fördelar mot lokala styrningsstrukturer.

Sverige i fokus

→ En restriktiv inställning till molnlösningar hänger i stor utsträckning samman med avsaknad av formella molnstrategier. I Sverige är dessa strategier vanligare inom privat sektor än offentlig vilket kan förklara den senares mer återhållsamma inställning till publika moln.

Vad anser du vara ditt ansvar som it-beslutsfattare när det gäller företagets hållbarhetsmål?



- A. Sätta och följa upp hållbarhetsmål för it-driften.
 B. Använda it- och analysverktyg för att stödja internt hållbarhetsarbete.
 C. Digitalisera processer för att nå hållbarhetsmål.
 D. Stödja utvecklingen av hållbara produkter/tjänster.
 E. Inget av alternativen är del av mitt ansvar.

När prioriteringar förändras riskerar hållbarhet att hamna i skymundan

Sverige i fokus

→ Svenska it-beslutsfattare anser i högre grad än sina motsvarigheter i Nordeuropa att hållbarhet är deras ansvar. Sverige ligger över genomsnittet på nästan alla indikatorer. I Sverige går man rentav emot en nedåtgående trend då en högre andel anger att deras strategier stöttar klimat- och sociala mål. Dessutom ökar behovet av hållbarhetskompetens. Samtidigt anger svenska it-beslutsfattare i mindre utsträckning hållbarhet som ett huvudsakligt fokus, vilket kan uppfattas som inkonsekvent eller ett tecken på att hållbarhet är mer integrerat i den övergripande it-verksamheten.

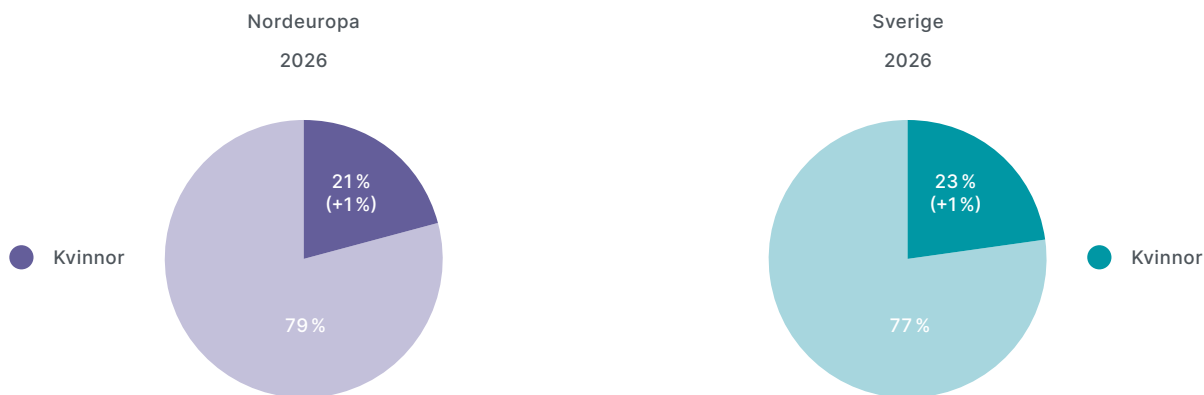
Antalet it-beslutsfattare som ser hållbarhet som en del av sitt ansvarsområde har sjunkit markant. Detta sker i en tid då andra prioriteringar dominerar, däribland säkerhetkrav. Vissa it-beslutsfattare kan också uppleva att hållbarheten numera är integrerad i verksamheten och inte längre ett separat ansvarsområde.

Den nedåtgående trenden syns inom alla listade hållbarhetsområden. Färre it-beslutsfattare inför eller följer upp hållbarhetsmål för it-driften, stödjer intern rapportering, digitaliserar processer för att uppnå hållbarhetsmål eller bidrar till hållbara produkter och tjänster. Nedgången har pågått tre år i rad, vilket tyder på ett fokusskifte snarare än lösryckta förändringar.

Organisationens mognad och storlek samt om it-beslutsfattare ingår i ledningen spelar roll när det gäller hållbarhetsansvar. Mognad i styrning och kapacitet stöttar ansvarstagande för hållbarhet.

Trenden väcker en viktig fråga: håller it på att glida för långt bort från hållbarhetsarbetet? It kan stärka sin position som möjliggörare genom datakvalitet, livscykelhantering, val av molnarkitektur och system som stöder korrekt rapportering utan att ta över hela ansvaret. På så sätt kan man höja hållbarhetsnivån samtidigt som man levererar operativa och kostnads-mässiga fördelar utan att lägga till nya fristående initiativ.

Hur många kvinnor arbetar på er it-avdelning?



Siffror inom parentes visar förändringen jämfört med förra året (procentenheter).

Högpresterande team uppstår inte av sig själva

Andelen kvinnor inom it-avdelningar i Nordeuropa ligger stadigt på omkring 20 till 21 procent. I sig själva indikerar dessa siffror varken mognad eller prestanda, men rapporter och studier – exempelvis McKinsey: Diversity matters even more, 2023 – visar att organisationer med mer balanserade team tenderar att uppvisa bättre resultat och högre mognad inom många områden.

Högpresterande team skapas genom medvetna ledarskapsval. Team med olika perspektiv hanterar svårigheter bättre, ifrågasätter antaganden mer effektivt och fördelar arbetsbelastningen på ett sätt som förhindrar flaskhalsar. Det blir allt viktigare i takt med att digitala miljöer blir mer sammankopplade och trycket på it ökar.

När organisationer breddar sitt rekryteringsspråk vittnar de om mer varierade profiler och bättre balans i teamen. Kommunikation är en annan grundläggande faktor. Team som

samordnar sig ofta och upprätthåller en tydlig, medveten kommunikation presterar bättre för att de arbetar med en gemensam förståelse och psykologisk trygghet.

Det finns skillnader mellan sektorer och organisationers storlek, men team med större andel kvinnor uppvisar oftare högre mognad och bredare samstämmighet. Det går inte att fastslå ett kausalt samband men siffrorna tyder ändå på att medvetet balanserade team får effekt för organisationernas prestationer.

Sverige i fokus

→ Sverige och Danmark utmärker sig när det gäller kvinnlig representation inom it. Det kan bero på en grundläggande stark inställning till jämställdhet och proaktiva initiativ inom teknikområdet. Sverige ligger i täten när det gäller nätverkande, synlighet och deltagande. Danmark kommer på andra plats och satsar på tvärvetenskapliga it-profiler. Tidiga systematiska utbildningsinsatser och rekrytering inom STEM-ämnena utgör grunden för Sveriges framsteg (Regeringen: "En STEM-strategi för Sverige", 2025, och Tech-Sverige: "STEM-strategin: Ett viktigt steg för att säkra framtidens kompetens", 2025).

SEB bygger högpresterande team genom tydlighet och mångfald

För att få till högpresterande team är det viktigt med tydlighet, kognitiv mångfald och att ge möjligheter till utveckling. Det menar Petra Ålund, HR-direktör på SEB sedan ett och ett halvt år, tidigare bankens CTO i drygt fem år.

I rollen som HR-direktör handlar Petra Ålunds arbete mycket om att bygga kultur och skapa förutsättningar för nya och gamla medarbetare att utvecklas.

– Fokus på utveckling är inte bara något vi säger, utan något vi verkligen menar. Trots att vi funnits i 170 år är vi en bank som alltid vill vara i framkant. Om en person är ointresserad av att utvecklas är nog inte SEB rätt bank att vara på. Just nu arbetar vi bland annat med att alla våra 19 000 anställda ska få chans att lära sig mer om AI.

Petra Ålund har lett många team genom åren, både inom och utanför it-sfären. För att få till högpresterande team tror hon på tillit och tydlighet.

– I dagens arbetsliv där utvecklingen går så fort jobbar vi med en hel del osäkerhet. Då blir det än viktigare med tydliga uppdrag, så att alla förstår vilken funktion de fyller. Då känns jobbet viktigare, vilket gör det roligare att gå dit. Detta gör det också lättare att prioritera, annars tar man ofta på sig mer jobb än vad man klarar av.

Även mångfald är viktigt – och här syftar inte Petra Ålund enbart på kön, utan snarare på att få in så många olika perspektiv som möjligt. Det kan handla om att rekrytera personer inom olika åldrar eller från olika länder, men även från flera typer av verksamheter – exempelvis ett litet bolag, en stor bankkonkurrent eller någon från



"Bra talanger drar till sig andra bra talanger. Och våga vara ärliga med vad ni anställer för, därigenom får ni in rätt typ av personal."

Petra Ålund, HR-direktör, SEB.

bilindustrin. Det finns en risk att produktleveranser landar fel om ens team eller bolag är för homogent. Här har Petra Ålund ett exempel från tiden som CTO.

– Vi jobbade med att ta fram ett mer digitaliserat bolåneförfarande, som vi trodde att många unga personer önskade, men det visade sig vara helt fel. Äldre personer, som redan hade köpt tre-fyra bostäder, ville ha en digitaliserad upplevelse. Yngre – potentiellt nervösa – förstagångsköpare ville gärna träffa oss fysiskt på banken. Med fler perspektiv i teamet hade vi nog haft lättare att förstå vår målgrupps behov.

Årets CIO Analytics-rapport visar att allt färre it-beslutsfattare ser hållbarhet som en del av sitt ansvar. Detta anser Petra Ålund vara konsekvensen av ett kortsiktigt tänk.

– För 20 år sedan var det inte många som baserade sitt val av bil

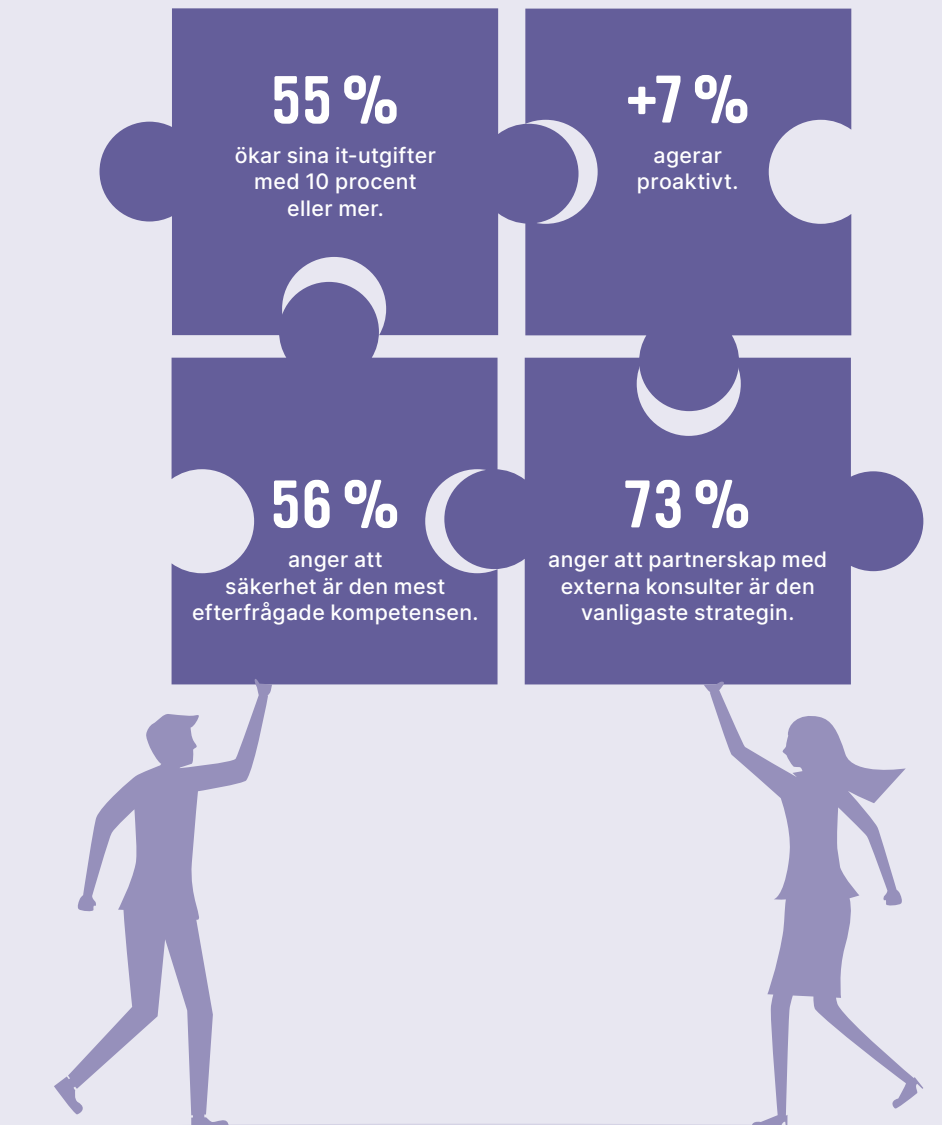
på hur lite energi den konsumerar, men det gör folk nu. Så kommer det att bli inom flera områden. Hypotetiskt: om jag vet att exempelvis Claude drar mindre energi än Chat GPT, varför skulle jag då välja Chat GPT? Bolag som skippar hållbarhetsfrågan får inte med den i sin produktutveckling, och riskerar att bli mindre intressanta för kunderna. Vi vet att hållbarhet är en differentierande faktor.

Petra Ålund avslutar med att ge några tips till CIO:er som vill bygga högpresterande team framåt:

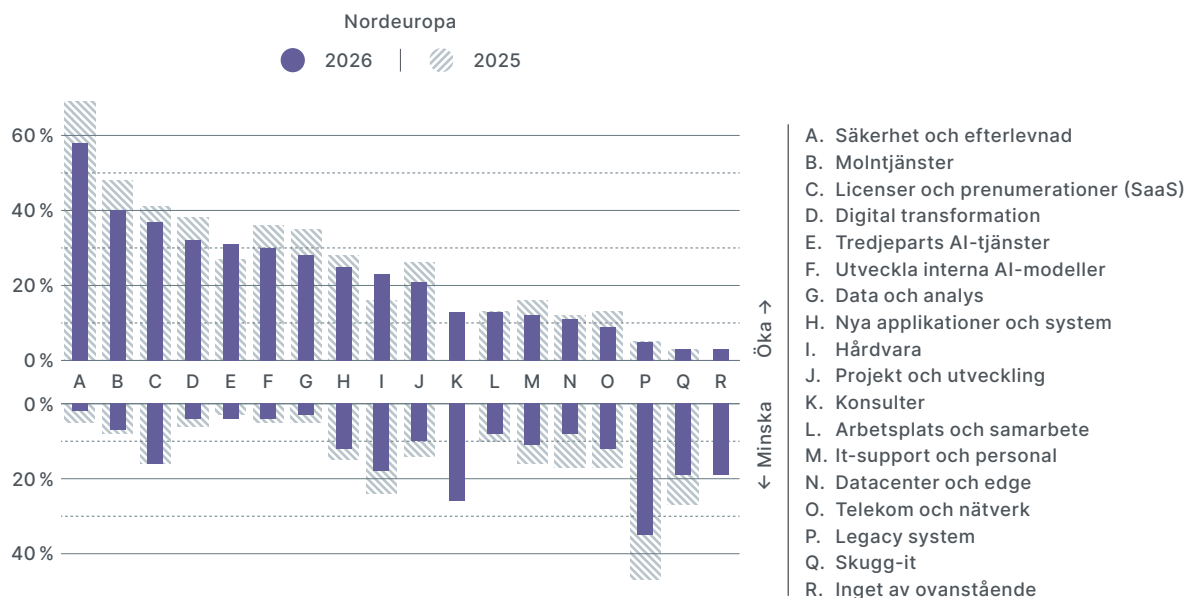
– Jobba nära din HR-chef. Ta tillsammans fram en employer branding-strategi över vilka sorters personer ni vill attrahera. Bra talanger drar till sig andra bra talanger. Och våga vara ärliga med vad ni anställer för; därigenom får ni in rätt typ av personal. Översälj inte en roll och lova inte för mycket – det kommer bara leda till att hen lämnar snabbt. ●

Skapa utrymme för det som spelar roll

Förmågan att utvecklas beror på människor och prioriteringar. Det här kapitlet tar upp hur utgifter förändras, vilka kompetensbehov som uppstår, tillgång på förmågor och hur it-organisationer utvärderas samt uppskattar sin proaktivitet



It-utgifterna kommer att öka/minska inom följande områden under året...



It-utgifterna ökar men prioriteringarna förändras

Sverige i fokus

→ It-utgifterna förväntas öka och fördelas över fler områden än tidigare. Säkerhet är den största budgetposten som driver mest kostnader i Sverige, 63 procent, påverkat av den rådande globala instabiliteten. Minskningen av utgifter för legacy system, 28 procent, är inte lika markant i Sverige som i övriga länder. Det beror på ett omfattande arv av gamla it-system i offentlig sektor. En tydligare standardiserad arkitektur är nödvändig för att minska framtida utmaningar kopplade till gamla system och inläsningseffekterna de medför.

It-budgetarna i Nordeuropa fortsätter att stiga och över hälften av organisationerna ökar sina utgifter med 10 procent eller mer. Utgiftsökningarna är dock koncentrerade till färre områden än förra året. Stigande priser på hårdvara, inflation och omprioriteringar tvingar it-beslutsfattare att fördela budgetarna mer selektivt.

Säkerhet och regelefterlevnad dominerar ökningarna. Ökade hot och nya regleringar tvingar organisationer att stärka kontroll, styrning och övervakning innan de skalar upp exempelvis automatisering eller AI.

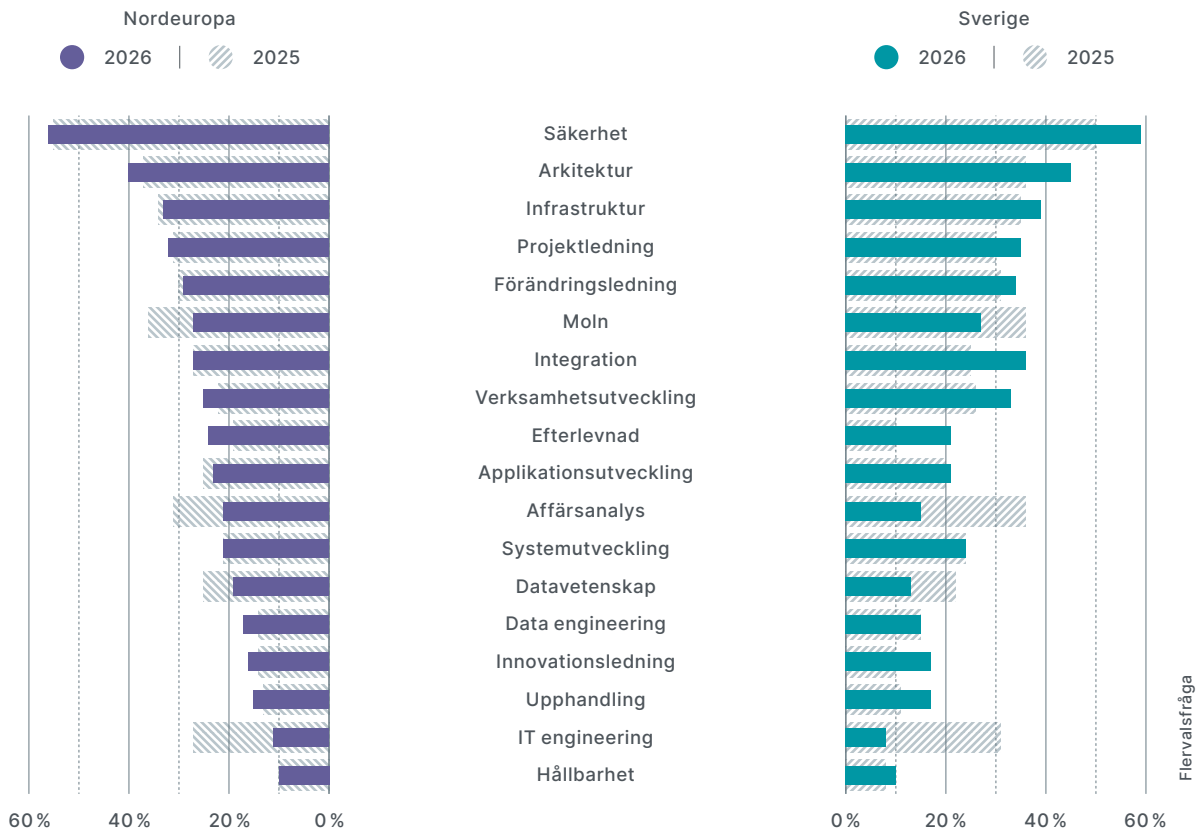
Utgifterna för AI ökar. Många organisationer befinner sig i ett tidigt mognadsstadium och investerar i det grundläggande såsom datakvalitet, styrning och säkerhet innan de kan realisera operativa avkastningar. (Det diskuteras vidare på sidorna 19 och 20.)

Utgifterna för molntjänster, prenumerationer och AI-verktyg från tredje part fortsätter att öka i takt

med leverantörsdrivna prisökningar. Samtidigt minskar konsultutgifterna, eftersom det ofta är den kategori som är lättast att skära ned på, även när det underliggande behovet kvarstår.

Utgifterna för legacy system minskar ytterligare. Enklare AI-drivna integrationer gör det frestande att arbeta runt åldrande plattformar, dock med risken att den tekniska skulden ökar och säkerheten försvagas på sikt.

Vilken/vilka it-relaterade kompetenser kommer er organisation att behöva inom de kommande 12 månaderna?



Kompetensutveckling, partnerskap och AI formar framtidens kompetensbehov

Säkerhet är fortfarande den mest efterfrågade kompetensen, då organisationer står inför regleringskrav och allvarligare hot. Arkitektur följer tätt efter, vilket speglar behovet av strategi, struktur och hållbara driftsmodeller inom molntjänster, AI och modernisering. Behoven är stora inom nästan alla kompetensområden, vilket visar hur hårt belastade it-avdelningarna har blivit.

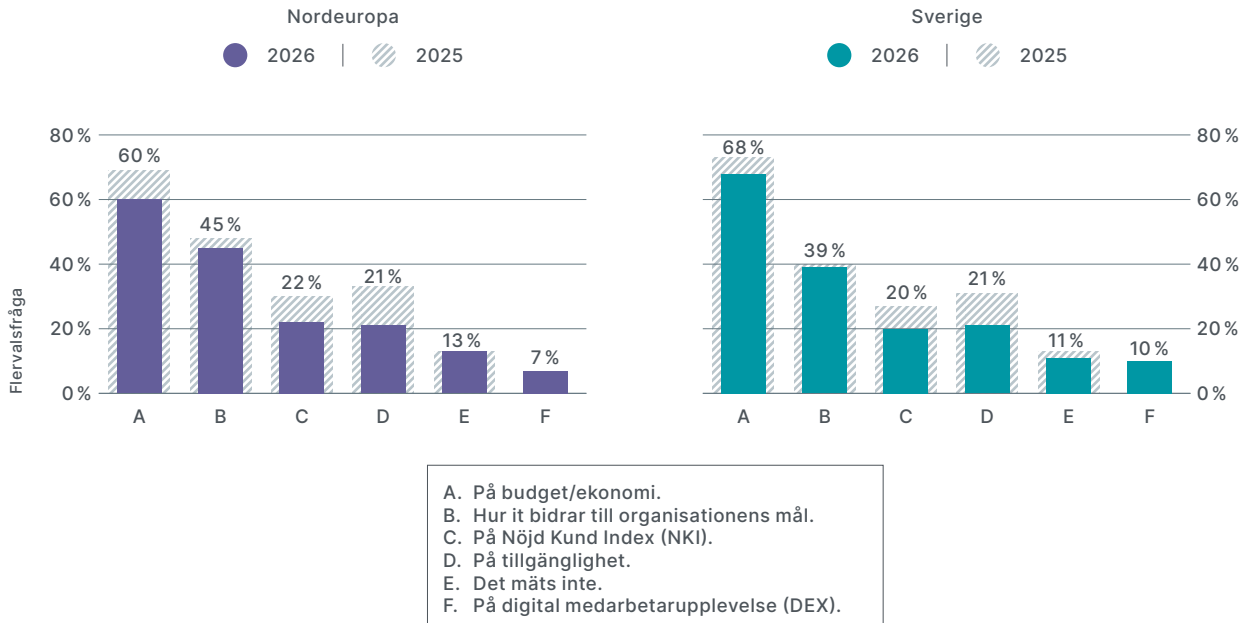
För att säkerställa framtida förmågor förlitar sig organisationer i hög grad på två strategier: partnerskap med externa konsulter och kompetensutveckling av befintlig personal.

Partnerskap hjälper till att fylla kritiska kompetensluckor, men då många planerar att minska konsultkostnaderna skapas en motsättning mellan kostnad och kapacitet. Kompetensutveckling blir avgörande när AI omformar roller, vilket ökar behovet av seniora arkitekter och säkerhetsexperter och minskar behovet av traditionella utvecklare. Beslutsfattande, kommunikation och förändringsledning är exempel på kompetenser bortom it som också behövs.

Sverige i fokus

→ Efterfrågan på kompetens är hög i hela Nordeuropa. Sverige har dock ett större behov av expertis inom centrala områden som säkerhet (59 procent), arkitektur (45 procent) och infrastruktur (39 procent). Klyftan mellan juniorer och seniorer förväntas öka i takt med att AI-tekniken förändrar traditionella nybörjarroller. På sikt kan det försvåra tillgången på kompetens. I Sverige framhålls rekrytering som en viktig strategi för att möta kompetensbehov.

Hur mäts och utvärderas er it-organisation?



It-avdelningens strategiska roll kräver nya sätt att utvärdera

Sverige i fokus

→ I Sverige utvärderas fortfarande många it-avdelningar inom både privat och offentlig sektor främst utifrån budget och ekonomiska resultat snarare än hur de bidrar till verksamhetens övergripande mål. Ett sådant fokus försvårar mätningen av det faktiska värde som it-investeringarna genererar. Det ser därmed ut att finnas ett tydligt behov av att förbättra hur svenska it-avdelningars insatser mäts och utvärderas.

Budget och ekonomi är fortfarande de vanligaste mätetalen för att utvärdera it-organisationer, trots ett växande behov av att visa på it-avdelningens bidrag till verksamhetens resultat. Mätningar kopplade till tillgänglighet, kundnöjdhet och affärsvärde har alla minskat jämfört med förra året, vilket väcker frågor om utvärderingsmetoderna håller jämna steg med de stigande förväntningarna på it.

Organisationer som ökar sina it-utgifter mäter mindre på budget och mer på värde. När en organisation väljer att göra betydande investeringar i it förväntas även ett strategiskt bidrag, inte bara kostnadskontroll. Organisationer som minskar sina it-utgifter ställs inför ökad budgetgranskning, minskad proaktivitet och ett fokus på kostnadsbesparingar snarare än verksamhetsutveckling. Det skapar en ond cirkel: budgetnedskärningar driver på budgetfokuserade

mätningar, vilket minskar affärs-effekten och kan leda till ytterligare nedskärningar.

Flera svar tyder på att it fortfarande ses som en supportfunktion snarare än en strategisk partner. Många it-beslutsfattare säger att de utvärderas utifrån kostnadseffektivitet snarare än resultat av transformation. Det handlar både om it-avdelningens interna rutiner och affärsenheternas mognad. Värdebaserade KPI:er kräver delat ansvar och organisationsstrukturerna är ofta inte redo för detta.

Nya KPI:er dyker upp, såsom mätvärden för digital medarbetarupplevelse, men användningen är fortfarande begränsad. Den underliggande utmaningen kvarstår: finansiella KPI:er är enkla att mäta medan värde, innovation och transformation är svårare att kvantifiera. Detta gap i mätmetoderna fortsätter att begränsa it:s strategiska roll.

Anser du att er it-organisation agerar proaktivt sett till verksamhetens behov?



- A. Ja, it-organisationen möter proaktivt verksamhetens behov.
 B. Nej, men it-organisationen går mot ett mer proaktivt arbetssätt.
 C. Nej, it-organisationen agerar mer reaktivt när det gäller vad verksamheten behöver.

Proaktiviteten ökar när it och verksamheten arbetar i samklang

Allt fler it-organisationer i Nordeuropa betraktar sig numera som proaktiva. Andelen har ökat jämfört med förra året och nära hälften anser att de förutser verksamhetens behov snarare än reagerar på dem. Ändå beskriver 22 procent fortfarande sin it-organisation som reaktiv.

It-beslutsfattare i ledningsgrupper bedömer sina organisationer som mer proaktiva, medan respondenter utanför ledningen eller utanför it-avdelningen är mer benägna att beskriva it som reaktiva. Det väcker frågor om gemensam förståelse: hur proaktivitet ser ut, om it kommunicerar sitt arbete tydligt och om verksamheten erkänner det värde som levereras. Uppfattningen formar förtroende och prioriteringar, vilket gör denna skillnad betydande.

Organisationer som ökar sina it-budgetar är mindre fokuserade på budgetmått och mer på värdeskapande. De beskriver också sig

själva som mer proaktiva. Organisationer som minskar sina it-utgifter tenderar att vara mer reaktiva, mer budgetstyrda och mindre benägna att investera i de resurser som krävs för framåtblickande it. (Läs mer om it-utgifter på sidan 30.)

It kan inte bli proaktiva på egen hand; affärsroller, processer och ägarstrukturer måste också utvecklas. Högre AI-mognad korrelerar också med hög grad av proaktivitet, troligen på grund av starkare grundläggande datastruktur, styrning samt erfarenhet av att koppla teknik till affärsvärde. Mänskliga förmågor spelar också roll: mod, kommunikation, inflytande och förmåga att ifrågasätta är väsentliga egenskaper för att gå från reaktivt beteende till strategiskt partnerskap.

Sverige i fokus

→ Sammantaget anser sig svenska it-beslutsfattare vara mindre proaktiva än sina motsvarigheter i övriga länder och andelen svenska it-beslutsfattare som säger sig vara reaktiva är något högre. Proaktiva organisationer mäter i högre grad hur it bidrar till verksamhetens mål. Dessutom finns det en koppling mellan hög AI-mognad och proaktivitet. Svenska it-organisationer som antar ett proaktivt och värde drivet tillvägagångssätt kan därmed fokusera mer på organisatoriskt värde än bara kostnadskontroll.

Utan it-investeringar kan verksamheten inte fungera

I Falu kommun ökar kraven på både säkerhet och digital utveckling samtidigt som kostnaderna stiger snabbare än budgeten. För it- och digitaliseringschef Anna Wickberg handlar arbetet om att prioritera rätt investeringar utan att tappa tempo i utvecklingen.

Aнна Wickberg ansvarar både för den löpande driften och det strategiska digitaliseringsarbetet i Falu kommun. Hennes roll omfattar allt från it-säkerhet och digital arbetsplats till utvecklingsinitiativ och AI. I nuläget präglas arbetet av ett tydligt investeringsfokus, inte minst inom säkerhet.

– Vi har en flerårig säkerhetsplan som vi följer, även om det inte går så snabbt som jag hade önskat. I år har vi fått ytterligare medel, vilket gör att vi kan införa fler säkerhetslösningar och driva projekt för att stärka säkerheten i våra verksamhetssystem.

Nya regelverk som cybersäkerhetslagen kräver samtidigt anpassningar inom kommunen.

– Vi var initialt ganska oroliga men insåg att vi redan har rutiner och strukturer på plats som bara behöver justeras, genom att exempelvis tidigarelägga vissa rapporteringssteg i våra incidentprocesser.

En annan central fråga är driften, och specifikt återinvesteringar i den digitala infrastrukturen. Ett område som blivit alltmer utmanande på grund av omvärldsläget.

– Prisbilder förändras extremt snabbt vilket gör att vi måste tänka om kring våra investeringsplaner för infrastrukturen.

Dessutom är investeringsutrymmet begränsat. Falu kommun får endast öka it-budgeten med 1,5 procent per år.

– Då kostnaderna ökar på alla områden, inte minst för hårdvara och säkerhetsrelaterad mjukvara, måste it-budgeten öka för att verksamheten ska fungera. Det enda område vi själva kan påverka är konsultkostnader och därför satsar vi mycket på intern kompetensutveckling. Förra året dubblerade vi utbildningsbudgeten vilket jag är väldigt stolt över.

Det ökade trycket har också förändrat dialogen med tjänstemannaledning och politiker som emellanåt kan

ifrågasätta varför kommuner satsar så mycket på it. Där menar Anna Wickberg dock att svaret är enkelt.

– Om vi inte fortsätter investera i it kan verksamheterna helt enkelt inte fungera, eftersom de är så beroende av digitala verktyg.

Investeringar och utveckling inom AI pågår parallellt, men med tydlig försiktighet.

– Potentialen är enorm, men vi måste arbeta försiktigt eftersom vi hanterar väldigt mycket känslig information.

Kommunen arbetar med flera parallella AI-spår men inväntar vissa strategiska beslut för mer klarhet. Anna Wickberg hoppas på att kommunsverige ska få mer stöd, från till exempel SKR och Digg, kring juridiska och strategiska vägval framåt.

– Ibland bygger vi lösningar som kan behöva byggas om i framtiden, men det är ändå bättre än att stå helt still.

Det viktiga, men även svåra, är att säkerställa att varje investering ger effekt. Anna Wickberg menar att kommunen behöver bli bättre på nyttokalkyler, att tydligt definiera investeringsvärdet och att följa upp efteråt.

– Oftast ligger nyttan inte hos it-avdelningen, utan i verksamheterna. Vi kan införa tekniken men det är verksamheterna som behöver ändra arbetssätt för att skapa värde. Mitt mål är att it ska sitta i passagerarsätet och hjälpa till med att visa vägen medan verksamheten styr. ●



"Potentialen är enorm, men vi måste arbeta försiktigt eftersom vi hanterar väldigt mycket känslig information."

Anna Wickberg, it- och digitaliseringschef, Falu kommun.



Förberedelser för framtiden: lärdomar och strategier

Denna rapport lyfter it-ledarskapets aktiva roll, där it-beslutsfattare uppmantras att fungera som strategiska partners till verksamheten. Den betonar vikten av att proaktivt hantera förändringar i omgivningen och använda ny teknik för att driva utvecklingen framåt.

Den ökade hotbilden sätter fingret på behovet av att öva på beredskapsplaner för att bygga upp verklig motståndskraft. Här behöver it, verksamhet och ledning samarbeta för att uppnå bästa möjliga beredskap.

När det gäller AI-användning har mognaden ökat men breddinföranden dröjer. För att ta nästa steg behöver it-beslutsfattare mäta resultat och koppla AI-satsningarna till affärs- och verksamhetsnytta i högre grad.

Verksamheten vänder sig allt oftare till it för vägledning vilket visar på behovet av att it-beslutsfattare tar ansvar för helheten.

Låt insikterna i denna rapport bli ett stöd och verka som inspiration på den fortsatta resan.

CIO ANALYTICS

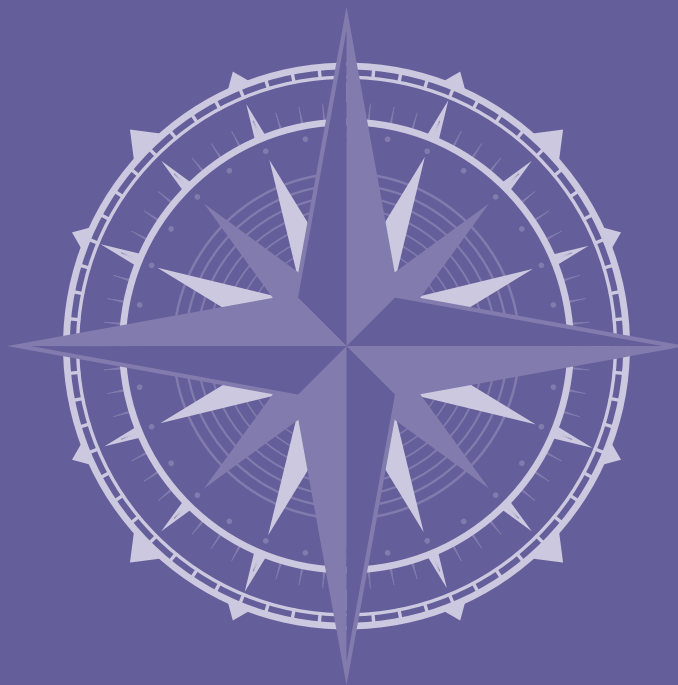
2026

AI

mognaden
ökar.

1/4

har ingen formell
molnstrategi.



+7%

agerar
proaktivt.

55%

ökar sina
it-utgifter.

ATERA