# VERKSAMHETSKRITISK DIGITAL INFRASTRUKTUR

Handbok för framtidssäkra lösningar för företag och organisationer

TELE2

FÖRETAG

# Dags att hitta balansen mellan tillgänglighet och kostnad

Digitaliseringen har påverkat oss sedan datorer började utvecklas på 1950- och 60-talen. Vi befinner oss nu i en tid av snabbt accelererande förändring där tekniker som Artificiell Intelligens (AI) och Internet of Things (IoT) och obegränsad uppkoppling lägger grunden för framtidens smarta samhälle. Ökad digitalisering kommer med fantastiska möjligheter, men också med nya utmaningar i form av sårbarhet, komplexitet och ökade krav på informationssäkerhet.

Mycket står på spel. En allt större del av en verksamhets tillgångar och värden idag är digitala, i form av tjänster och produkter, kunskap, data, information och algoritmer i våra system. Uppkoppling och IT är i många fall en förutsättning för en verksamhets existens. Utmaningen är att hitta rätt balans mellan å ena sidan tillgänglighet och öppenhet, å andra sidan kostnaden för säkerhet och skydd - och att ständigt ompröva och anpassa lösningen till en föränderlig omvärld.

Vi har tagit fram denna handbok som en hjälp i arbetet med att optimera den verksamhetskritiska digitala infrastrukturen. Baserat på våra samlade erfarenheter av nätverk, digitalisering och informationssäkerhet bjuder vi på ovärderliga insikter om teknikval i förhållande till kostnadsnivå. Vårt mål är att bidra till utvecklingen av värdeskapande, effektiva och hållbara produkter och tjänster samt att skapa i alla avseenden framtidssäkra organisationer.

# Innehållsförteckning


**Digitalisering är samhällskritisk** **4**
Verksamheter blir alltmer beroende av att digitala tillgångar är tillgängliga 5
Digital kommunikationsteknologi samhällskritiskt 6
Varför investera i något som inte händer? 7
Varför uppstår incidenter? 8
Välj strategi för att undvika och hantera avbrott 9
Kontinuitetshantering är ett pågående arbete 11
Undvik avbrott i en kedja av samband 11

**Att skapa en digital infrastruktur med hög tillgänglighet** **13**
Alternativ för placering av digitala tillgångar 13
Allt vanligare med hybrida molnlösningar 14
Hållbarhet som drivkraft för molnet 15
Högre krav på nätverket 16
Lokala nät 17
Accessnät 17
Redundans och diversitet vid behov 18
Vad händer när din fasta eller mobila uppkoppling når operatörens nät? 19
Fysiskt distribuerat nät - WAN 20
Logiskt distribuerat nät - SD-WAN 21
Tillgänglighetsnivåer kan säkras med SLA 22
Utmaningen är att hantera balansgången 22

**Vi vill hjälpa er skapa en verksamhetskritisk digital infrastruktur** **24**
Lokal infrastruktur 24
Access 24
Wide Area Network (WAN) 24
Hantering av digitala tillgångar 25
Hållbarhet är vårt fokus 25

**Kundcase** **27**
Besikta flyttade från molnet till Malmö 27
Postnords mål - fossilfritt, resurseffektivt och en nollvision för arbetsskador 28

# Digitaliseringen är samhällskritisk

Det har gått mer än ett halvt sekel sedan de första datorerna började utvecklas på 1950- och 60-talen och det vi kallar digitalisering inleddes. I dag lever vi i en tid av snabbt accelererande förändring, i ett hyperuppkopplat samhälle med tekniker som Internet of Things (IoT), Virtual Reality (VR), moln och 5G - och en allt kraftfullare Artificiell Intelligens (AI).

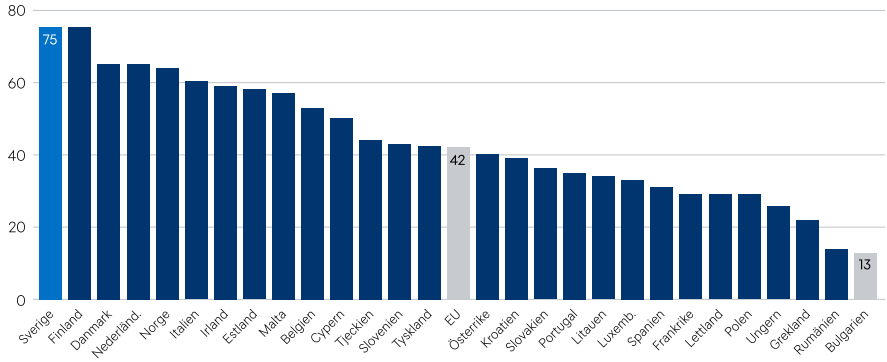
Digitaliseringen har många sidor, bland annat som möjliggörare och drivkraft för ett effektivt, hållbart och jämlikt samhälle. Inom EU har EU-kommissionen satt upp ambitiösa mål för medlemsländernas digitalisering fram till 2030 och slagit fast att "...den europeiska vägen mot en digitaliserad ekonomi och ett digitaliserat samhälle handlar om solidaritet, välstånd och hållbarhet, baserat på medborgarnas och företagens egenmakt, samtidigt som säkerheten och resiliensen säkerställs för Europas digitala ekosystem och försörjningskedjor."

Med hjälp av ett särskilt index, Digitalt Intensitets Index (DII), mäts EU-medlemsländernas digitala mognad, baserat på 12 identifierade komponenter:

- Köper fast Internetuppkoppling med hastighet minst 30 Mb/s nedströms
- Använder någon typ av social media
- Mer än 50 procent av de anställda använder dator med uppkoppling till Internet inom arbetet
- Använder någon typ av molntjänst
- Har affärsstödssystem för att dela information mellan funktioner
- Har kundhanteringssystem (CRM)
- Köper Contact Center-lösning
- Använder minst två typer av sociala media
- Använder IoT
- Företag med e-handel som uppgår till minst 1 procent av totala omsättningen

- Företag med webbhandel som uppgår till minst 1 procent av totala omsättningen varav B2C webbhandel utgör minst 10 procent av totala webbhandeln
- Använder någon typ av AI-teknologi

I ramverket "Path to the Digital Decade" fastställs målet att 2030 ska mer än 90 procent av små och medelstora företag i medlemsländerna ha uppnått minst basnivån av digitalisering och 75 procent ska använda moln, AI och Big data. Sverige ligger bäst till när den senaste mätningen gjordes 2021 (se fig.1).




**Figur 1. Digitalt Intesitetsindex, 2021** *(Källa: Eurostat 2022)*

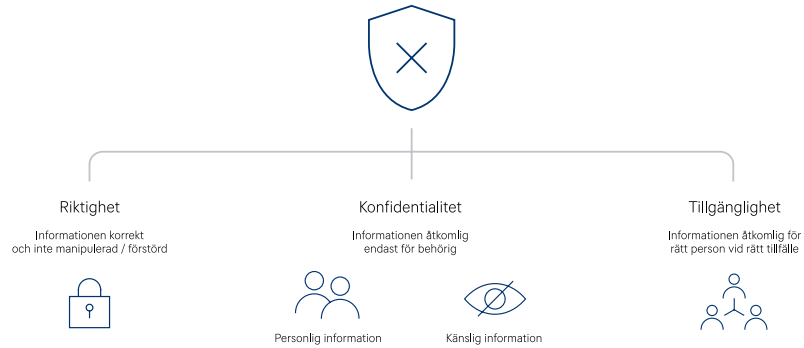
## Verksamheter blir alltmer beroende av att digitala tillgångar är tillgängliga

Med ökad digitalisering kommer stora möjligheter, men också nya utmaningar i form av ökad sårbarhet och komplexitet. Ju mer vi digitaliserar desto viktigare blir informationssäkerhet (även om informationssäkerhet självklart gäller all information oavsett om den är digital eller ej).

En stor del av en verksamhets eller organisations värde består idag av digitala eller immateriella tillgångar. Det kan vara digitala produkter, information, medarbetarnas kunskap, kund- eller produktdata, algoritmer eller varumärket i sig. Uppskattningsvis är 70-85 procent av ett företags informationstillgångar

digitala (*Källa: Eurobank 2017*). Beroendet av it- och informationssystem är allt starkare, dels internt då de knyter samman verksamhetens tillgångar system och processer, men i allt högre grad också externt i relation till hela ekosystemet av leverantörer, kunder, partners och myndigheter. Den digitala infrastrukturen är både verksamhetskritisk och samhällskritisk och måste skyddas därefter.

Tillämpad informationssäkerhet handlar om att data och information måste skyddas så att de inte råkar i fel händer, förstörs eller förvanskas. I sammanhanget brukar man tala om Riktighet, Konfidentialitet och Tillgänglighet (se fig.2). Det gäller att se till att data och information är korrekt och inte ändrad eller förstörd (Riktighet), att säkerställa att bara rätt personer har tillgång till data och information medan obehöriga stängs ute (Konfidentialitet), och att rätt data och information finns tillgänglig vid behov (Tillgänglighet).




**Figur 2. Informationssäkerhetens delar** *(Källa: Säkerhetspolisen, 2020)*

## Viktigt att säkra samhällsbärande infrastruktur

Inom EU uppmärksammas informationssäkerhetsfrågorna i det så kallade NIS-direktivet, The Directive on Security of Network and Information Systems (EU) 2016/1148. NIS beskriver åtgärder och krav för att skapa och bibehålla en hög säkerhetsnivå i nätverk och informationssystem i hela EU. Reglerna omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster. Med samhällsviktiga tjänster avses tjänster som är viktiga för att upprätthålla en kritisk samhällelig eller ekonomisk verksamhet.

En svensk NIS-aktör som drabbas av en incident i ett informationssystem eller

ett nätverk, vilken i sin tur leder till en störning i leveransen av en samhällsviktig funktion eller digital tjänst, ska rapportera incidenten till CERT-SE. Det är Sveriges nationella incidenthanteringsfunktion (Computer Emergency Response Team) som lyder under MSB (Myndigheten för Samhällsskydd och Beredskap) och som har i uppdrag att stötta samhället i arbetet med att hantera och förebygga it-incidenter. MSB sammanställer och analyserar informationen i de rapporter som kommer in.

Rapporterna skickas även vidare till den NIS-tillsynsmyndighet som berörs, exempelvis Finansinspektionen, Livsmedelsverket eller Post och Telestyrelsen (PTS). På så vis får vi mer kunskap om de incidenter som drabbar svenska leverantörer av samhällsviktiga funktioner och digitala tjänster samt en strategisk helhetsbild av incidenterna som äger rum och hur de påverkar det svenska samhället i stort.

I Sverige har Tele2 en tydligt samhällsbärande funktion, i egenskap av leverantör av kommunikationsinfrastruktur, telefoni och nätverkstjänster. Därmed ställs höga krav på hur vi säkerställer tjänsterna till våra kunder. Att arbeta strukturerat och metodiskt med informationssäkerhet är en förutsättning för att kunna bedriva en säker verksamhet. Som stöd använder vi ISO 27001, ett vedertaget ledningssystem som används av oss och många andra.

## Varför investera i något som inte händer?

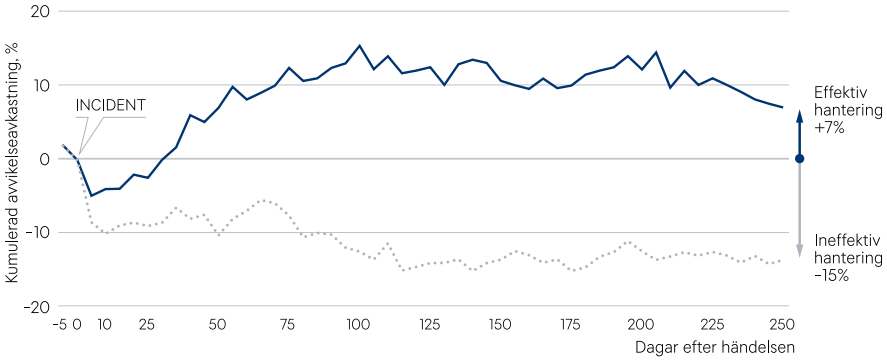
Kanske är sannolikheten för ett avbrott eller en incident låg, men effekten för företaget eller organisationen kan likväl bli kritisk.

Att förlora uppkoppling eller data till följd av en incident kan vara förödande. Även kortare avbrott kan orsaka stora skador i form av intäktsbortfall, förlorad information eller skada på verksamhetens rykte. För snart tio år sedan, i maj 2013, låg webbsidan amazon.com nere i 30 minuter, vilket resulterade i nära 30 miljoner dollar i förlorade intäkter, eller 66 240 dollar per minut (*Källa: Forbes Magazine*). Men även ett betydligt mindre företag än Amazon kan skadas allvarligt av ett ofrivilligt avbrott.

För varje bolag som får sin inkomst via digitala kanaler, exempelvis en e-handel eller ett företag som lever på digital kommunikation, kan det dagliga inkomstbortfallet räknas ut som företagets årsomsättning delat med 365. Ett företag som omsätter 300 miljoner kronor årligen skulle således förlora 800 000 kronor i genomsnitt på en dags avbrott. Mindre organisationer är dessutom ofta sämre

rustade för att hantera eventuella konsekvenser av bortfallet än de stora. Förluster kan komma i fler former än inkomstbortfall. Ett avbrott under ett kundsamtal kan exempelvis få kunden att tro att ditt företag inte är tillräckligt stabilt eller pålitligt. Om problem med uppkopplingen gör att företaget eller organisationen förlorar viktig information kan det medföra stora problem.

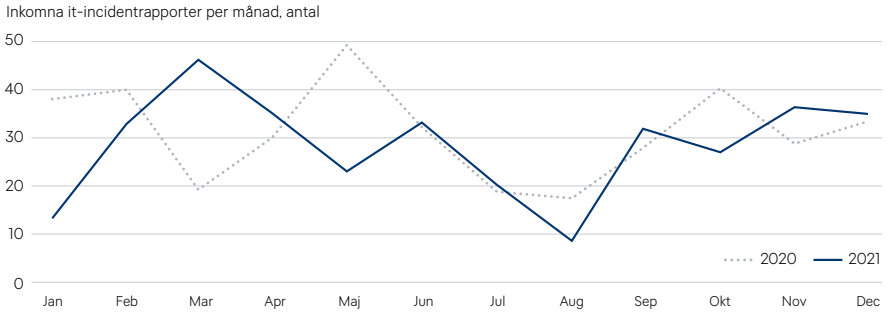
Företag som går igenom kriser kan grovt sett delas in i två kategorier – de effektiva som återhämtar sig snabbt via krishantering respektive de som är ineffektiva och återhämtar sig långsamt eller inte alls (se fig.3). Forskning från University of Oxford visar att de förstnämnda på sikt ökar sitt börsvärde, medan de i den andra kategorin tappar kraftigt. Många oförberedda organisationer överlever inte alls. Det handlar alltså inte bara om att undvika avbrott (vilket är närmast omöjligt) utan också om att ha processer på plats för att effektivt kunna hantera dem.




**Figur 3. Varför investera i något som kanske aldrig händer?** *(Källa: The Impact of Catastrophes on Shareholder Value, Rory F. Knight & Deborah J. Pretty, Templeton College, University of Oxford, 1996)*

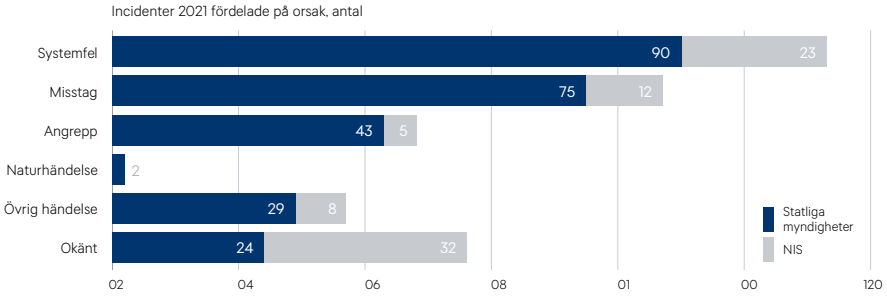
## Varför uppstår incidenter?

Under 2021 inkom 343 rapporter om it-incidenter till MSB (se fig.4). Av dessa var 261 rapporter från statliga myndigheter och 82 från leverantörer av samhällsviktiga och digitala tjänster. Detta kan jämföras med 374 inrapporterade incidenter under 2020 där 286 kom från statliga myndigheter och 88 från NIS-leverantörer, det vill säga en viss minskning. Antalet är dock bara en del av problematiken, vissa incidenter skapar större skada än andra. Det finns således ett tydligt värde i att arbeta mot en noll-vision.




**Figur 4. Rapporterade incidenter 2021**
*(Källa: Myndigheten för Samhällsskydd och Beredskap [MSB] – årliga it-incidentrapportering 2021)*

Enligt MSB:s årliga it-incidentrapportering 2021 (se fig.5) var den i särklass vanligaste orsaken till de incidenter som rapporterades in systemfel följt av misstag och sedan angrepp. Så har det sett ut de senaste åren. En bidragande orsak till detta kan vara att komplexiteten i lösningarna har ökat. Därför är det förebyggande arbetet, exempelvis kartläggning av informationstillgångar, samt arbetet med framtagande av processer, metoder och policier alltmer viktigt.




**Figur 5. Orsaker till samhällskritiska incidenter**
*(Källa: Myndigheten för Samhällsskydd och Beredskap [MSB] – årliga it-incidentrapportering 2021)*

## Välj strategi för att undvika och hantera avbrott

Hur gör man då för att komma i gång med informationssäkerhetsarbetet och se till att det blir effektivt och ändamålsenligt?

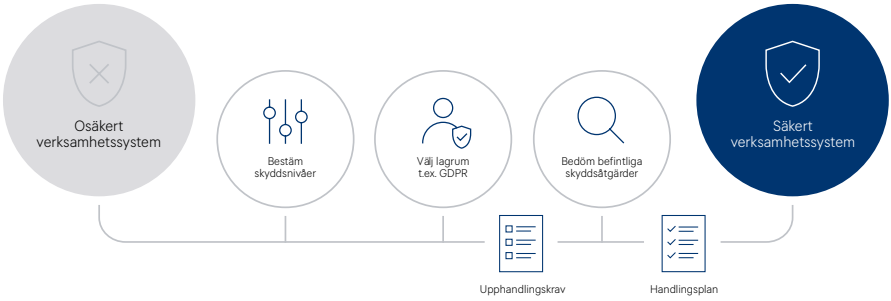
Först gäller det att skaffa sig en god förståelse för organisationen och dess mest kritiska processer, delprocesser och system. I en mindre organisation, med få anställda och ett överskådligt antal it-system, behöver en sådan kartläggning inte vara så komplicerad utan den borde kunna skötas av ett fåtal personer. I en större organisation med fler system och mer komplexa processer måste fler individer involveras. Detta för att säkerställa att alla aspekter och beroenden – strategiska, tekniska och rent operativa – fångas upp och beaktas.

Sedan gäller det att identifiera vilken information som stöttar processerna och hanteras i systemen för att det i nästa steg ska vara möjligt att klassificera informationen utifrån relevans, krav på säkerhet och tillgänglighet.

KLASSA är ett självskattningsverktyg för informationsklassning som är skapat för Sveriges Kommuner och Regioner (SKR) (se fig.6). För andra organisationer finns även en öppen version av KLASSA. Klassningen ifråga kan gå till som följer;

**Steg 1.** Börja med att bedöma säkerhetsrisken kopplad till information i verksamhetens it-system på en skala från "försumbar" till "synnerligen allvarlig" och beakta de tre perspektiven Konfidentialitet, Riktighet och Tillgänglighet vad avser verksamhetens krav på information och data.

**Steg 2.** Undersök om det finns tvingande lagar och regelverk att förhålla sig till. Alla verksamheter måste exempelvis följa dataskyddsreglerna vid behandling av personuppgifter (GDPR). Det gäller oavsett om det är en offentlig myndighet, ett privat företag, en förening eller någon annan typ av verksamhet. NIS-direktivet ställer krav på säkerhet i nätverk och informationssystem och omfattar




**Figur 6. Informationsklassning är en metod som hjälper verksamheten att välja rätt åtgärder för att skydda information** *(Källa: Klassa, Sveriges Kommuner och Regioner)*

leverantörer av samhällsviktiga tjänster och vissa digitala tjänster. Det kan även finnas andra relevanta lagar att förhålla sig till, beroende på bransch eller verksamhet, exempelvis Patientdatalagen eller Arbetsmiljölagstiftningen.

**Steg 3.** Gör en självskattning av hur verksamheten ligger till.

**Steg 4.** Skapa en handlingsplan baserat på en sammanvägning av verksamhetens krav på tillgänglighet och säkerhet, befintliga åtgärder och eventuella gap.

**Steg 5.** Slutligen gäller det att åtgärda det som krävs. Det kan exempelvis handla om att bygga upp nya lösningar för att minska risken för avbrott, eller om att införa processer för att hålla igång verksamheten på en tolerabel nivå i händelse av it-avbrott. Det sistnämnda kallas kontinuitetshantering, eller på engelska Business Continuity Management.

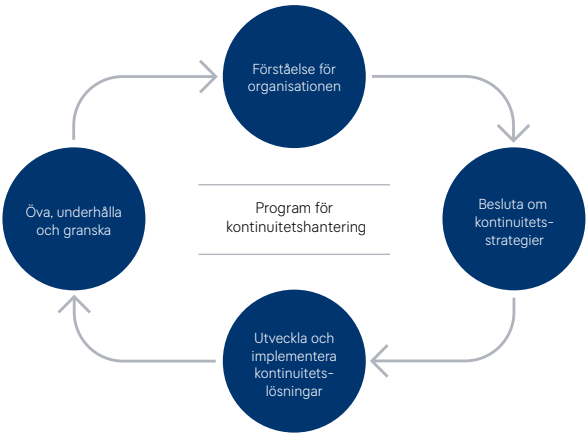
## Kontinuitetshantering är ett pågående arbete

För bästa resultat följer även arbetet med it-kontinuitethantering några väl definierade steg. Först och främst gäller det förstå vilka processer som är mest verksamhetskritiska och vilken data och information som har högst affärsmässigt värde för verksamheten. Att metodiskt utveckla och strukturera upp de data och den information som finns i organisationen, på ett enhetligt och övergripande sätt ger en god grund för det fortsatta arbetet. När all information är kartlagd och på plats blir samband och beroenden tydliga och ledningen kan enas om vad som är acceptabla respektive oacceptabla konsekvenser för verksamheten i händelse av ett ofrivilligt avbrott.

Standarden ISO 22301 (se fig.7), erbjuder ett stöd för organisationer oavsett storlek för att arbeta med kontinuitetshantering på ett systematiskt och strukturerat sätt. På så vis blir din verksamhet bättre rustad för att hantera eventuella hot och incidenter.

## Undvik avbrott i en kedja av samband

Ingen kedja är starkare än sin svagaste länk. Just detta är de starka beroenden som på senare år har uppstått mellan affärsverksamhet, it-system och informationshantering ett tydligt bevis på – i synnerhet när leverantörer kunder och partners ingår i samma intrikata ekosystem. En liten incident på ett håll kan få oanade och ibland extrema konsekvenser någon helt annanstans.




**Figur 7. ISO 22301** *(Källa: SIS, Svenska Institutet för Standarder)*

Kraven på att verksamheter och tjänster ska kunna upprätthållas även i händelse av avbrott och haverier ökar. Det krävs dock mycket planering och omfattande investeringar för att kunna erbjuda en sådan likhet under i stort sett alla förhållanden. Närhetsprincipen sätts på prov när den som äger data inte längre hanterar den och leverantören kanske befinner sig ett halvt jordklot bort eller i molnet. Här finns ett antal tydliga utmaningar.

# Att skapa en digital infrastruktur med hög tillgänglighet

Många organisationer vill själva kunna kontrollera sina verksamhetskritiska tillämpningar och sin säkerhet. Samtidigt är investeringar i ny teknik förknippade med kostnader och resurser – inte bara idag utan också över tid.

Som vi nämnt tidigare beror avbrott i systemen på en rad olika saker och det finns olika tekniker för att förhindra dem. I denna handbok tittar vi i detalj på hur vi kan förhindra avbrott som beror på systemfel, misstag och/eller naturhändelse.

Att undvika avbrott på grund av angrepp är ett annat stort område som beskrivs inom området cybersäkerhet, men som vi lämnat utanför denna gång.

## Alternativ för placering av digitala tillgångar

Med tanke på att en verksamhets värde i allt högre grad utgörs av digitala tillgångar (se sidan 7) är det affärsmässigt viktigt att ha en strategi för hur och var dessa tillgångar ska hanteras. Målet är att få till en lösning som är tillgänglig, användarvänlig, robust och säker. Historiskt sett lagrades data lokalt och även tillämpningar kördes lokalt. Över tid har distribuerade lösningar tillkommit och även möjliggörande kommunikationstjänster.

Att använda molntjänster för lagring och hantering av digitala tillgångar är för många ett attraktivt alternativ, inte minst ur tillgänglighetssynpunkt. Eftersom all åtkomst till systemen sker via uppkoppling har användaren full tillgång till information och data oavsett var han eller hon befinner sig: Samtidigt är upplevelsen av tjänsten att information finns på den egna datorn.

Det finns flera sorters molnlösningar att hålla reda på:

- **Publika moln** underhålls och driftas av en extern leverantör, som Microsoft Azure, Amazon Web Services eller Google Cloud. Publika molntjänster är

flexibla och mångsidiga för organisationer med komplexa behov. Tjänsterna är tillgängliga för alla verksamheter och användaren delar server med andra verksamheter, medan leverantören tar fullt ansvar för support och säkerhet.

- **Privata moln** är enbart tillgängliga för den egna organisationen. Det innebär att infrastrukturen finns på ett privat nätverk och att funktioner och resurser kan utvecklas och anpassas specifikt utifrån behov och förutsättningar. Privata moln är en bra lösning för företag och organisationer som hanterar känslig eller affärskritisk information, eller som behöver ha extra kontroll på sin it-lösning.
- **Hybrida moln** kombinerar privata moln, publika moln och ett eget datacenter i en sammanslagen lösning. Kombinationen ger fördelarna av det publika molnet, där användaren kan överlåta drift och ansvar till en extern leverantör, men samtidigt behålla tryggheten i den egna it-miljön för känslig information eller delar som är svåra att flytta av tekniska skäl.
- **Multi-molnlösningar** innebär att verksamheten använder två eller fler privata och/eller publika molntjänster från flera olika leverantörer. Den här typen av lösning används allt oftare av företag och organisationer som vill dra nytta av fördelarna med flera olika molntjänster.

## Allt vanligare med hybrida molnlösningar

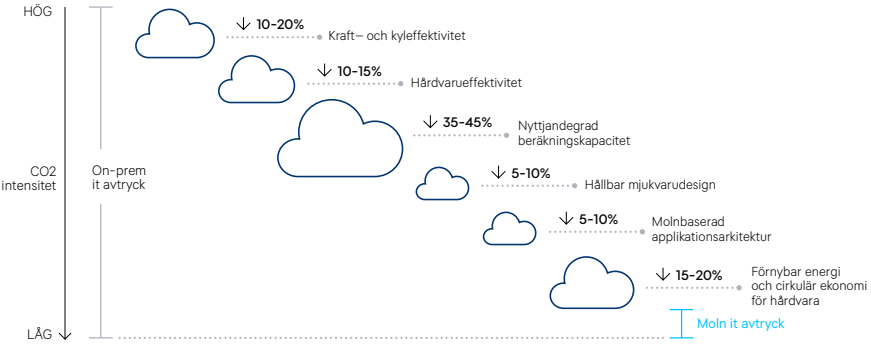
Idag är det vanligt att företag och organisationer satsar på en kombination av molntjänster. Den mest kostnadseffektiva lösningen för de flesta verksamheter är en kombination av privata och publika moln, hybridmoln.

Enligt analysföretaget Gartner kommer 80 procent av företagen ha stängt ner sina datacenter och övergått till moln- eller colocation-lösningar till år 2025. Inställningen hos många nordiska företag är att använda molnlösningar där det är relevant. Det vill säga inte inte molnet först, “cloud first”, utan “cloud where it makes sense” (*källa: DC Nordic Multicloud Survey*).

Som vi såg tidigare i MSB:s statistik är den vanligaste orsaken till avbrott systemfel tätt följt av misstag. Att anlita en tredje part för driften av datacenter, privata moln eller hybridmoln kan minska risken för att misstag begås. Eftersom dessa leverantörer har molndrift som kärnverksamhet har de byggt upp relevant kompetens och rutiner som de också kan utveckla och upprätthålla över tid.

## Hållbarhet som drivkraft för molnet

En annan drivkraft för övergången till molntjänster är hållbarhet i form av minskad energianvändning och reducerade koldioxidutsläpp. Världens omkring nio miljoner datacenter står för drygt 1 procent av världens energianvändning, enligt International Energy Agency, IEA. Samtidigt pekar flera studier på att övergången till molntjänster bidrar aktivt till att minska koldioxidutsläppen jämfört med lokala lösningar "on prem" (se fig.8).



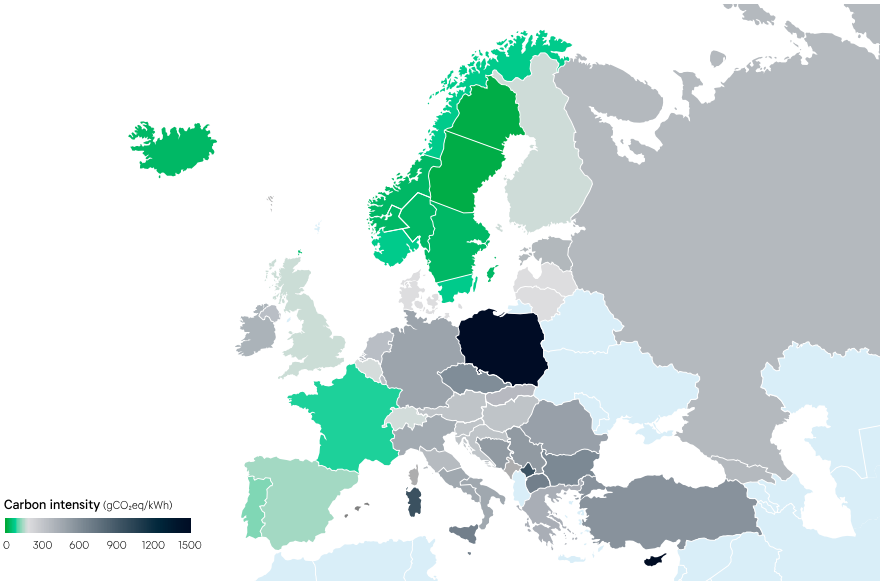

**Figur 8. Minskat miljöavtryck med molnet** *(Källa: The Green behind the Cloud, Accenture 2020)*

Genom att nyttja fysisk infrastruktur och kapacitet mer effektivt uppnås besparingar på mellan 45-70 procent. Utöver det tillkommer möjligheten att använda överskottsvärme från datahallarna till uppvärmning av andra lokaler liksom att återanvända uppvärmt kylvatten.

Det finns även potential att minska miljöpåverkan direkt via mjukvarudefinierade tjänster (software defined services). Ett bra exempel är Amazons CodeGuru, en machine learning-tjänst som hjälper företaget med att identifiera mjukvara som inte är optimal. Från 2017 till 2018 ökade Amazon sin applikationseffektivitet i så hög utsträckning att nyttjandegraden av deras processorkraft (CPU, Central Processing Unit) ökade med 325 procent. Därmed kunde man minska antalet instanser för att hantera onlinehandel vid peak.

När Tele2 gick från traditionell datadrift till software defined datacenter ledde den rena hårdvarueffektiviseringen till en 30 procent energibesparing.

$CO_2$ avtrycket kan även minskas via nyttjande av förnybar energi (se fig.9).




**Figur 9. EU elkonsumtion $CO_2$ intensitet** *(Källa: Electricity Maps, 2023)*

Eftersom andelen förnybar energi varierar stort inom t ex Europa så kan valet av land där datacenter som realiserar molnet fysiskt finns vara avgörande.

I Sverige arbetar Energimyndigheten för ett hållbart energisystem, som förenar ekologisk hållbarhet, konkurrenskraft och försörjningstrygghet. Tillsammans med ett flertal aktörer har man investerat 50 miljoner i forskningsprojektet Cloudberry Datacenters vars syfte är att utveckla kunskapen om energi och resurseffektiva datacenter. Det övergripande målet är att effektivisera energianvändningen. Forskarna kommer utvärdera tolv delprojekt i fyra år. Några av de frågor som söker svar är om det går att bygga datacenter annorlunda för att minska energiåtgången. Om spillvärmen kan användas till något nyttigt. Och vilken typ av mjukvaruarkitektur som behövs för att öka energieffektiviteten.

## Högre krav på nätverket

I takt med att fördelarna med molntjänster blir alltmer uppenbara, ökar också kraven på organisationernas nätverk. Särskilt som många företag och organisationer sitter med blandade hybridlösningar med inslag av olika moln och egna system. Vad ska man tänka på ur ett tillförlitlighetsperspektiv? Hur skapar man

en verksamhetskritisk digital infrastruktur som kopplar ihop verksamhetens alla delar, system och data? Vilka tillgänglighetskrav finns? Och hur hanteras risker? Allt detta påverkar hela lösningen och avgör hur driftsäker den blir. Nedan listar vi några olika nätverksvarianter;

**Lokala nät**
För det lokala nätverket, LAN (Local Area Network),i de egna lokalerna finns olika alternativ för uppkoppling av utrustningen, både fast och trådlöst, exempelvis via WiFi eller Privat 5G-mobilnät.

Organisationen kan välja att ha sina data och applikationer i en egen datahall, i en infrastruktur som kan vara fysiskt helt skild från Internet (en så kallad on prem-lösning). Då ansvarar man oftast själv för drift och skalskydd. Viktigt att tänka på är att säkerställa ordentliga batteribackuper samt att bygga upp backupvägar och täckning där det behövs över tid. (Olika typer av trådlösa lokala nät beskrivs mer i detalj i vår handbok "Framtidens trådlösa uppkoppling".)

**Accessnät**
Kraven på omedelbar tillgång till en organisations applikationer "as a service" ökar exponentiellt. Både internt och bland utomstående. Fler människor, enheter och avancerade media-tillämpningar tävlar om åtkomsten – en utveckling som drivs på av molnteknologierna.

Det är företagets WAN (Wide Area Network) som får ta smällarna. Dessvärre är det sällan optimerat för en så snabbt växande trafik. Ett WAN är ett nätverk som kopplar samman två eller flera affärsplatser och som använder samma protokoll som internet för dataöverföringen (IP, Internet Protocol). Åtkomsten till ett WAN kan vara fast eller trådlöst.

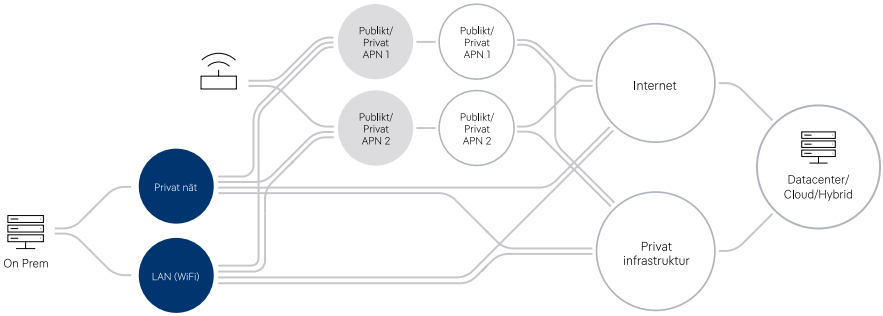
Viktiga förmågor för att kunna möta den ökade efterfrågan på applikationer är förutsägbarhet och prestanda. Både i molnet och det egna datacentret spelar förutsägbarhet och prestanda hos applikationerna en avgörande roll för användarupplevelsen. För att applikationerna ska kunna användas optimalt måste nätverken förstå trafikflödena. Att enbart flytta trafik från A till B är inte nog.

En fast uppkoppling kan realiseras på flera olika sätt. Den enklaste varianten är en fast uppkoppling över Internet. Det innebär att WAN-kommunikationen går över det öppna Internet, där det inte går att garantera bandbredd eller erbjuda kvalitetsklasser (QoS, Quality of Services). Ovanpå Internet-förbindelsen skapar man då krypterade tunnlar för sitt WAN.

Nästa steg är att köpa en kapacitetstjänst (IP-VPN) som ger en specifik bandbredd inom tjänsten. Ett IP-VPN är i regel uppbyggt med garantier i form av kapacitetsgaranti och kvalitetsklasser (QoS) Den mest exklusiva varianten är att hyra dedikerad fiber. Dedikerad fiber innebär att man har fri tillgång till förbindelsen och att den egna utrustningen därmed är det som sätter begränsningen för hur mycket kapacitet och hur många kvalitetsklasser man kan få. Dedikerad fiber kan fungera bra om det endast är ett fåtal adresser. Om antalet anslutningspunkter ökar blir det svårt att bygga ett väl fungerande WAN utan att komplexiteten ökar exponentiellt och att kostnaden blir mycket hög.

## Redundans och diversitet vid behov

För Tele2 och andra svenska operatörer som tillhandahåller samhällskritiska tjänster ställs enormt höga krav på att kunna säkerställa leveransen till sina kunder. Men incidenter kan ändå ske och för den som behöver ta höjd erbjuds alternativet att bygga in redundans, det vill säga ett parallellt system som tar över om ett annat ligger nere. En organisation som är i behov av riktigt hög tillgänglighet för sin mobila uppkoppling kan exempelvis bygga in två eller flera parallella mobilabonnemang i samma utrustning – skulle ett nät gå ner kopplas man i så fall över till ett annat. Den extra kostnaden för dubbleringen kan definitivt vara motiverad när det gäller kritiska tillämpningar (se fig.10).




**Figur 10. En potentiell systemlösning med redundans och diversitet** *(Källa: Tele2)*

För organisationer med fast uppkoppling och höga tillgänglighetskrav finns också möjligheten att bygga in redundans. En variant är att bygga en primär och en sekundärförbindelse på olika platser, med olika kraftförsörjning och olika åtkomst (även inom organisationens lokaler). Det är också möjligt att ha en

mobil 4G/5G-uppkoppling som en av förbindelserna. För en mobil uppkoppling går det inte att garantera tillgänglighet eller bandbredd eftersom den nyttjar publika nät. Oavsett lösning bör den primära och sekundära förbindelsen - om möjligt är - ha likvärdig kapacitet. Detta för att inte tillgängligheten till system ska påverkas i händelse av ett eventuellt avbrott i den primära förbindelsen.

Om man behöver högre tillgänglighet än vad redundans kan ge, kan man använda en strategi som kallas diversitet. Det innebär att man använder två eller flera fysiskt separata alternativ med olika lösningar för elförsörjning och anslutningar. Till exempel två olika nätleverantörer, en fast och en mobil uppkoppling, eller två olika mobiloperatörer som backup ifall en av dem skulle ha störningar eller avbrott i sitt nätverk.

Utbyggnaden av 5G-nätet, som bland annat levererar hög kapacitet, medför nya möjligheter För att få en maximal bandbredd i ett 5G nät krävs att man befinner sig i ett område där 5G körs på hög frekvens. Dock medför hög frekvens att täckningen, speciellt inomhus, blir sämre. Därför rekommenderas en lokal 5G-accesspunkt med extern antenn som kan monteras utomhus. (Läs mer om mobil uppkoppling i vår handbok “Framtidens trådlösa uppkoppling”.)

## Vad händer när din fasta eller mobila uppkoppling når operatörens nät?

I ett mobilt nät lämnar datatrafiken nätet via ett så kallat Access Point Name (APN), en passage, en gateway, mellan mobilnätet och ett annat datornätverk – som det publika Internet eller privat infrastruktur. APN avgör vilken typ av nätverksanslutning som ska skapas, till exempel vilka IP-adresser som ska tilldelas till enheten, och vilka säkerhetsmetoder som ska användas. Alla mobiloperatörer har publika APN men det går att beställa ett Privat APN, det vill säga en egen kanal i operatörens nät. Med ett Privat APN definierar du vart din datatrafik ska kopplas, till exempel mot ett publikt nät, dedikerade VPN eller ett privat IP-nät. Ett privat APN kan också ge anslutning till ett företags intranät så att dess resurser (program, filer, skrivare) blir tillgängliga för mobila enheter.

Om du har en fast uppkoppling så kopplas din router, Customer Premises Equipment CPE, till din tjänsteleverantörs Provider Edge (PE)-router som kopplar till leverantörens IP-nät.

För transport mellan olika accesspunkter, APN eller Provider Edge, används

IP-transportnät, som är nationella eller internationella. En leverantör av privat IP-infrastruktur byggt på fiberoptik, ibland kallat IP-stamnät, kan garantera tillgänglighet på olika sätt genom inbyggd redundans i sin lösning. Men det kräver att alla accesspunkter är direkt anslutna till den privata IP-infrastrukturen.

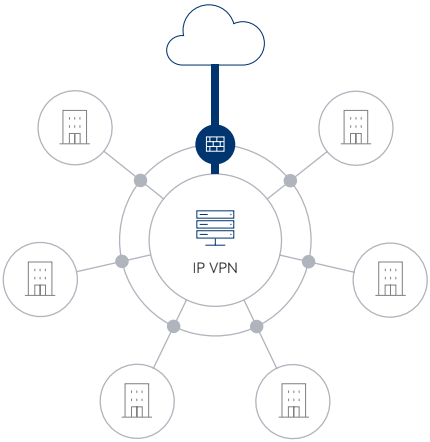
Slutligen: För vissa verksamhetskritiska applikationer kan man köra både accessnät, applikation och data lokalt på plats, en så kallad on-prem lösning, vilket vi nämnt tidigare. Det kan vara relevant av tillgänglighetsskäl eller i verksamheter med extremt korta fördröjningskrav, till exemple autonoma fordon, eller autonoma mobila robotar i en produktionsanläggning.

## Fysiskt distribuerat nät - WAN

Många organisationer vill inte bara koppla ihop sina geografiska verksamheter utan också koppla upp sig mot olika molntjänster. Det finns idag lösningar för att ansluta sig direkt till publika molntjänster från vissa nät via privat infrastruktur. Det är en lösning som passar bra för exempelvis IoT-tillämpningar (Internet of Things) där uppkopplade enheter skickar data direkt till molnet, till en applikation internt eller en extern tjänst. I dessa fall ansvarar den som driver den privata infrastrukturen för kopplingen direkt till de olika molntjänsterna vars accesspunkter kan befinna sig på olika platser geografiskt.

Ett annat alternativ är att lämna över trafiken till Internet, men då finns ingen som garanterar tillgängligheten.

Säkrare och stabilare är att skapa en krypterad förbindelse, eller tunnel, över internet i form av ett virtuellt privat nät, VPN som använder IP-protokollet. Tekniken kallas IP VPN och den används ofta i kombination med Multi Protocol Label Switching, MPLS (vilket tekniskt sett innebär att man använder etiketter istället för IP-adresser i routningen av datapaket). IP VPN säkerställer att data inte avlyssnas eller förvanskas under överföringen. MPLS-tekniken är utvecklad för att ge hög kapacitet, servicenivå och tillförlitlighet. I och med att IP VPN levereras på en dedikerad förbindelse erhålls hög prestanda och flexibilitet med minimal fördröjning. För att öka tillgängligheten och skydda tjänsten i ett IP VPN är redundans inbyggd. Tekniska, geografiska och ekonomiska ramar sätter gränserna för vad som är möjligt. Det finns olika möjligheter att ansluta till ett IP VPN, dedikerad fast uppkoppling, via mobilnät (och Privat APN) eller med IP Sec över Internet. Varje alternativ har olika egenskaper. Ett IP VPN kräver konfiguration i operatörens nät samt hårdvara i varje ändpunkt (se fig11).




**Figur 11. Systemöversikt IP VPN lösning** *(Källa: Tele2)*

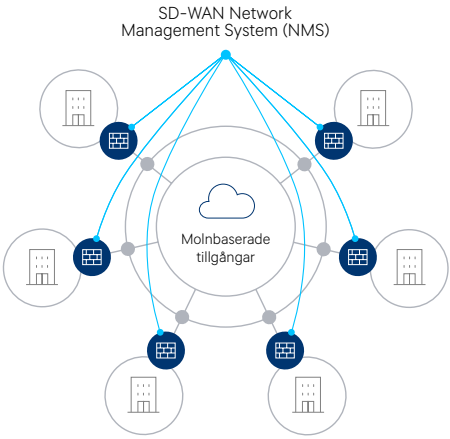
Ett VPN använder ofta en publik gateway för att koppla upp. Fokus ligger på att säkra konfidentialitet via kryptering, det vill säga inte på att säkerställa tillgänglighet. Det är ett vanligt sätt att skapa en säker uppkoppling till verksamhetens it-miljö för anställda som arbetar utanför organisationens lokala nät.

## Logiskt distribuerat nät - SD-WAN

För många organisationer har nätverkstrafiken successivt flyttat till molnet, från att tidigare huvudsakligen ha gått mellan lokala kontor eller servrar i egna datacenter. Om internettrafiken då måste passera en central punkt används inte resurserna i WAN:et på ett optimalt sätt, eftersom det i sin tur kan skapa flaskhalsar och leda till ökade kostnader.

Ett ny teknik för att bygga logiskt distribuerade lösningar är SD-WAN, Software Defined Wide Area Network. Den stora skillnaden mellan IP VPN och SD-WAN är att i ett VPN kopplas en användare eller en annan typ av ändpunkt till en specifik punkt i nätverket, medan ett SD-WAN skapar länkar mellan flera nät som i sig kopplar till flera ändpunkter. SD-WAN läggs ovanpå ett underliggande IP-nätverk, det spelar ingen roll vilket, och därför kan många olika typer av anslutningstjänster och tekniker användas. Du väljer själv om du vill köra utan eller med underliggande anslutningstjänster (se fig.12).

SD-WAN brukar implementeras med dedikerad hårdvara vid ändpunkterna i kombination med ett system för nätverkadministration, Network Management




**Figur 12. Systemöversikt SD WAN lösning** *(Källa: Tele2)*

System, som i realtid visar exakt hur nätet används, vilka applikationer som drar kapacitet och hur accesserna till eventuella molnleverantörer levererar. Det gör att du enkelt kan optimera, justera och också felsöka lösningen.

Jämfört med traditionellt IP VPN där utrullningen av en eller flera verksamhetsställen tar relativt lång tid, utgår SD-WAN istället från att så snabbt som möjligt få upp WAN:et. Dessutom kan hastigheten och kapaciteten ofta ändras av kunden i Network Management Systemet.

## Tillgänglighetsnivåer kan säkras med SLA

SLA står för Service Level Agreement – ett serviceavtal som anger vilken kvalitetsnivå en leverans ska hålla. SLA:et reglerar vanligtvis vilken tillgänglighet systemet ska ha, hur många gånger ett fel får förekomma under en given tidsperiod, hur lång tid det får gå innan felavhjälpning påbörjas samt hur snabbt felet ska vara åtgärdat.

En SLA-nivå kan räknas om i hur lång maximal nedtid som garanteras, det vill säga hur länge en digital tillgång, exempelvis ett betalningssystem, en app eller ett administrativt system maximalt blir otillgängligt för användaren. I tabellen nedan syns några av de vanligast förekommande nivåerna som referens och respektive maximal nedtid beräknat på tillgänglighet 24/7 (se tabell 1).

| SLA | Nedtid/dag | Nedtid/vecka | Nedtid/månad | Nedtid/år |
|---|---|---|---|---|
| 99,99% | 8,6s | 1m 0,48s | 4m 21s | 52m 9,8s |
| 99,9% | 1m 26s | 10m 4,8s | 43m 28s | 8t 41m 38s |
| 99,0% | 14m 24s | 1t 40m 48s | 7t 14m 41s | 3d 14h 56m 18s |

**Tabell 1. Nedtid i förhållande till SLA nivå** *(Källa Tele2)*

## Utmaningen är att hantera balansgången

För varje organisation är det en balansgång mellan värdet av att minska negativ påverkan och kostnaden för att skydda digital infrastruktur för att uppnå önskad tillgänglighet. Här har vi gjort en enkel översikt som indikerar vilken typ av tillgänglighetsökande teknologi man bör ha i förhållande till den konsekvensnivå man beslutat vara godtagbar baserat på klassningen för respektive digital tillgång (se tabell 2).

| Konsekvensnivå* | Måttlig | Allvarlig | Betydande |
|---|---|---|---|
| Föreslagen Service Level Agreement (SLA) nivå | Best effort | 99,0% | 99,9% |
| Accesslösning | Fast eller mobil internetanslutning | Redundant | Redundant med diversitet |
| Transport | Internet | Privat IP | Privat IP med redundans |
| WAN | IP Sec VPN | IP VPN/SD-WAN | SD-WAN |
| Datalagring | On prem | 1 datacenter med redundans | Metrocluster – 2 datacenter |
| Kostnad | Låg | Medel | Hög |

*Nivå av negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ

**Tabell 2. Tillgänglighetsökande teknologier för olika konsekvensnivåer** *(Källa Tele2)*

Som framgår av tabellen finns det möjligheter med olika lösningar, men ju högre tillgänglighet man vill garantera desto högre bli kostnaden så det är viktigt att göra en medveten avvägning.

# Vi vill hjälpa er att skapa en verksamhetskritisk digital infrastruktur

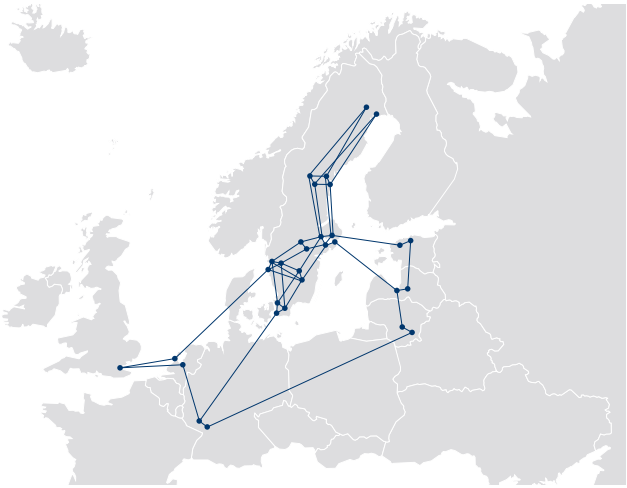
Tele2 Företag säkerställer din organisations verksamhetskritiska digitala infrastruktur genom kontinuerlig driftövervakning enligt det serviceavtal din verksamhet behöver.

**Lokal infrastruktur**
Vi kan hjälpa dig med både trådbundet och trådlöst lokalt nät, LAN. Det trådlösa kan vara baserat på WiFi eller Privat 5G.

**Access**
Vi levererar fast internetaccess via vårt eget fiberoptiska IP-stamnät som har direkt förbindelse med alla stora internetoperatörer och garanterar en bandbredd från 10 Mbit/s till 10 Gbit/s. IP-nätet är byggt med optiska fiberringar för att erbjuda bästa möjliga tillgänglighet, hög kapacitet med korta fördröjningar och hög genomströmning. Vi levererar också mobil bredbandsaccess 4G/5G som primär access eller som mobil redundans om din verksamhet har kritiska behov av tillgänglighet. Tele2s mobilnät täcker 99,9 procent av Sveriges befolkning och 90 procent av Sveriges yta, med ständigt pågående utbyggnader och förbättringar.

**Wide Area Network (WAN)**
Eftersom vi transporterar all vår nättrafik (tv, mobilsamtal, internet, VPN) är kraven på driftsäkerhet och redundans extremt höga. Vi använder dubbla 100 Gigabits-trianglar mellan Göteborg, Stockholm och Malmö (se fig.13). Det innebär att vi kan tappa upp till tre delsträckor utan någon som helst påverkan på trafiken.

Tele2:s datanät produceras över egen fiber och våglängdssystem vilket innebär att vi snabbt kan uppgradera kapaciteten i vårt stamnät. Från Sverige har vi fysiskt separerade fiber mot centrala Europa samt tre fysiskt separerade förbindelser till USA:s östkust, där vi byter trafik med ledande operatörer. Många



**Figur 13. Tele2s fibernät** *(Källa: Tele2)*

organisationer har idag distribuerat sin verksamhet på flera orter. Oavsett hur många ni är eller var ni befinner er kan vi hjälpa er att jobba som en gemensam organisation. Vi erbjuder både IP VPN och SD-WAN lösningar – era behov är avgörande.

### Hantering av digitala tillgångar

Vår Hybrid Cloud-lösning består av en portfölj av flera produkter som är skalbara, standardiserade och tydligt prissatta. Tjänsten levereras i vårt eget säkra Tele2 Cloud eller via publika moln som Microsoft Azure. Tele2 Företag står för hantering, förvaltning och drift oavsett om hela tjänsten kommer från oss eller via en underleverantör. Vi har kompetensen, rutinerna och erfarenheterna för att hantera verksamhetskritisk data, och vi driftar idag it-system för flertalet samhällsviktiga funktioner där kontroll är högsta prioritet.

Vi levererar Tele2 Cloud från några av Nordens bästa datacenter och serverplattformar, utrustade med rigorös tillträdeskontroll, brandskydd, strömförsörjning och kyla enligt N+1-principen.

### Hållbarhet är vårt fokus

Vi vill använda vår teknologi, uppkoppling och kunskap för att utveckla produkter och tjänster som bidrar till effektivitet och hållbarhet. Vårt nät kan bidra till att övervaka och bevara resurser och därmed öka effektivitet och minska kostnader.

Vår teknik kan övervaka produktionsflöden och optimera processer så att det går åt mindre resurser och energi. Med vår samhällsinfrastruktur i botten lägger vi också grunden för framtidens uppkopplade företag och organisationer och det smarta samhället i stort.

# Kundcase

## PostNords mål - fossilfritt, resurseffektivt och en nollvision för arbetsskador för de anställda

För att nå sina ambitiösa mål satsar PostNord på fortsatt digital transformation, en framåtblickande molnstrategi och ett optimerat och modernt nätverk.

Bakom fasaden påminner PostNords paketterminaler om godshanteringen på en flygplats. Men i stället för väskor är det paket som snabbt susar förbi i ett komplicerat nät av gummiklädda rullband, för att sorteras och skickas in på rätt band till rätt slutdestination. En förutsättning för att maskineriet ska fungera är ett säkert, flexibelt och snabbt datanätverk längs hela logistikkedjan av fordon, terminaler och omkring 8 000 utlämningsställen och ombud.

### Kundcase Postnord

- Tele2 Företag förser PostNord med en helhetslösning för all datakommunikation i Norden. Här ingår WAN och LAN i Sverige och Danmark, inklusive lokala nätverk på alla utlämningsställen i Sverige.

- För fem år sedan tog Tele2 Företag även över ansvaret för driften av hela nätverket. Inom ramen för tjänsten Network as a Service hyr PostNord nu all nätverksutrustning som switchar och accesspunkter, medan Tele2 Företag garanterar tillgängligheten

- E-handeln ökar kraftigt och antalet paketleveranser slår rekord. PostNords ledning har därför identifierat fortsatt digital transformation som en av de viktigaste byggstenarna för framtiden. Här spelar it-infrastrukturen och nätverket en viktig roll.

- Liksom andra delar av näringslivet och industrin behöver PostNord förhålla sig till en explosion av molnbaserade tjänster och applikationer samt inflödet av enorma datamängder från allt fler uppkopplade sensorer och enheter. Detta ställer också nya krav på nätverken.

Läs mer: **https://www.tele2.se/foretag/content/kundcase/postnord**

# Besiktas digitaliserade bilbesiktning kräver stabila flöden och säker drift

Stabil leverans, ökad tillgänglighet och bättre ekonomi. Det blev resultat när Besikta flyttade sina servrar till Tele2 Företags datacenter i Limhamn utanför Malmö.

Besikta Bilprovning grundades 2013 med målet att förnya bilbesiktningsbranschen som fram till 2010 var ett statligt monopol. Med 186 stationer på 152 orter i Sverige, från Luleå i norr till Simrishamn i söder, från Gotland i öst till Orust i väst, har Besikta idag Sveriges största stationsnät. Besikta erbjuder årlig kontrollbesiktning och nyregistrering av bilar, mc, lastbilar och släp plus en rad kringtjänster.

## Kundcase Besikta

- Tusentals fordonsbesiktningar genomförs av Besikta varje dag, i ett flöde som är fullt ut digitaliserat och som ställer extremt höga krav på stabilitet och säker drift. Allt från bokning till besiktning sköts via nätet. Det är bara kvittot och protokollet som skrivs ut på papper, men de lagras också digitalt.

- Besiktningspersonen är utrustad med en handdator som kopplar upp sig mot Transportstyrelsen via en app för att hämta och skicka data i realtid, innan och efter besiktningen. Betalningen hanteras digitalt via en extern leverantör.

- Tele2 Företag fick tidigt ansvar för kommunikationsinfrastrukturen, i form av LAN och WAN som tjänst till alla servicestationer samt fast och mobil telefoni.

- Sedan i december 2018 hanterar Tele2 Företag också driften av samtliga verksamhetskritiska system för Besikta. Hela IT-miljön ligger numera på servrar i Tele2 Företags ISO27001-certifierade datacenter i Limhamn utanför Malmö som använder 100 procent förnybar energi vilket bidrar till Besiktas högt ställda mål inom miljömässig hållbarhet genom effektivt nyttjande av IT-infrastruktur.

- Sedan i december 2018 hanterar Tele2 Företag också driften av samtliga verksamhetskritiska system för Besikta. Hela it-miljön ligger numera på servrar i Tele2 Företags ISO27001-certifierade datacenter i Limhamn utanför Malmö som använder 100 procent förnybar energi vilket bidrar till Besiktas högt ställda mål inom miljömässig hållbarhet genom effektivt nyttjande av it-infrastruktur.

Läs mer: **https://www.tele2.se/foretag/content/kundcase/besikta**

## Behöver du hjälp i ditt val?

Det finns många faktorer att beakta när du väljer digital infrastruktur till verksamheten. Viktigast av allt är dock att det är organisationens unika behov och krav som ska styra. Oavsett vilken lösning du väljer är det den digitala infrastrukturen som skall stödja verksamhetsprocesserna, i stället för att organisationen ska anpassa sig till it-lösningen.

Hos Tele2 Företag finns anpassade kommunikationstjänster och lösningar för företag och organisationer. Vill du veta mer eller få rådgivning av våra experter? Välkommen att **kontakta oss**.

TELE2
FÖRETAG

TBUS2537_2302