Säkra elektroniska kommunikationstjänster

– en vägledning till användarorganisationer

2024–08–21
Rapport: PTS-ER-2024:23

Inledning

Vårt samhälle knyts samman genom elektronisk kommunikation. Vi människor når varandra, våra digitala tjänster och vår information genom den. De digitala och fysiska system som finns överallt i samhället kommunicerar också ofta elektroniskt med varandra. Att detta är säkert - att det fungerar som det ska - är därför helt avgörande för samhällets funktion.

Kommunikationen sker framför allt via allmänt tillgängliga tjänster för elektronisk kommunikation så som internetanslutning, telefoni, meddelandetjänster, VPN och andra tjänster för informationsöverföring. Tjänster tillhandahålls av operatörer och används av såväl privatpersoner som företag, kommuner, myndigheter och andra organisationer. Det finns drygt 600 operatörer i Sverige som via elektroniska kommunikationsnät tillhandahåller ett brett utbud av allmänt tillgängliga elektroniska kommunikationstjänster.

Egenskaperna i de elektroniska kommunikationstjänster som används, liksom hur de används, är viktiga för säkerheten hos en organisation. Detta är i många fall en del av organisationens bredare arbete med cybersäkerhet.

Målet för den här vägledningen är att den ska bidra till ett säkrare samhälle genom att hjälpa organisationer att identifiera och tillgodose sina behov av säkerhet vid inköp och användning av elektroniska kommunikationstjänster. Vägledningen riktar sig till personer som arbetar med kravställning, inköp, säkerhet, beredskap och kontinuitetsplanering hos företag, kommuner, myndigheter och andra organisationer.

Post- och telestyrelsen (PTS) som tagit fram den här vägledningen är den myndighet som bevakar områdena elektronisk kommunikation och post i Sverige. PTS arbetar genom samverkan, främjande insatser, reglering och tillsyn för att hela Sverige ska ha tillgång till säker och tillgänglig kommunikation.

Det är viktigt att ha i åtanke att denna vägledning inte är ett facit för vilken säkerhet din organisation behöver eller vilka typer av tjänster som ni ska köpa. Alla organisationer är olika både vad gäller behov och förutsättningar. Och marknaden för elektronisk kommunikation är stor och i ständig utveckling. Vår ansats är att beskriva ett antal aspekter hos vanliga typer av tjänster som har betydelse för säkerheten, vägleda på övergripande nivå i hur organisationens behov kan klargöras samt ge exempel på områden som kan vara relevanta att ställa krav på vid ett köp.

Innehållsförteckning

Disposition

Vägledningen inleds med en sammanfattning, som följs av fem kapitel.

I kapitel 1 introducerar vi ett antal centrala begrepp.

I kapitel 2 beskriver vi på en övergripande nivå hur några vanliga typer av elektroniska kommunikationstjänster fungerar och belyser några av de aspekter som påverkar säkerheten.

I kapitel 3 beskriver vi hur ni kan gå till väga för att identifiera organisationens behov av säkerhet.

I kapitel 4 beskriver vi hur ni kan planera för att uppfylla era behov av säkerhet.

I kapitel 5 fördjupar vi ett antal områden som kan vara relevanta att ställa krav på vid köp av elektroniska kommunikationstjänster.

I slutet av vägledningen finns en lista med lästips och en ordlista med viktiga begrepp.

Avgränsningar

Vägledningen har en bred ansats men har ett antal tydliga avgränsningar:

- Den omfattar bara allmänt tillgängliga elektroniska kommunikationstjänster, inte organisationens eventuella egna elektroniska kommunikationsnät som till exempel nät inom ett kontor.
- Vägledningen omfattar inte heller organisationens egna digitala system. Det är alltså inte en vägledning inom hela det breda området cybersäkerhet.
- Materialet ska stödja i inköpsprocessen, men beskriver inte i detalj hur inköp eller offentlig upphandling ska genomföras.
- Vägledningen är inte specifikt utformad för krisberedskap utan belyser i stället områden som är allmänt relevanta för säkerhet.

Sammanfattning

En säker elektronisk kommunikationstjänst kan sägas vara en tjänst som fungerar trots oönskade händelser. Vad som är rätt nivå av säkerhet för er beror på vilken verksamhet ni bedriver, vilket syfte tjänsten fyller i er verksamhet, hur ni använder den, vilka värden som ska skyddas mot vilka hot och vilken risk ni kan acceptera.

Det som behöver skyddas i en tjänst är dess tillgänglighet, konfidentialitet, riktighet och autenticitet. Vad som är viktigt varierar mellan olika användningsfall. För att åstadkomma säkerhet på ett effektivt sätt behöver ni sannolikt prioritera mellan dessa olika aspekter. Det behöver också göras en avvägning mellan förmågan att stå emot påfrestningar (robusthet) och förmågan till återhämtning och att klara av förändringar (resiliens).

Några faktorer som generellt är viktiga för att åstadkomma en säker tjänst är att det finns ett visst överskott av resurser (redundans) och inbyggda olikheter (diversitet) i produktionen, inklusive i elförsörjningen. Andra viktiga faktorer är operatörens generella säkerhetsarbete och att komplexiteten hålls på en hanterbar nivå. Det är en god idé att sätta er in i hur de fundamentala egenskaperna för en elektronisk kommunikationstjänst påverkas av hur den produceras, till exempel olika former av access eller transport.

För att ta reda på vilken säkerhet ni behöver måste ni ha en god kännedom om hur elektronisk kommunikation används i er verksamhet. Med det som utgångspunkt kan ni sedan göra en bedömning av vilka värden – i bred bemärkelse - som riskeras för er organisation om olika aspekter av säkerheten skulle brista. Innan ni tittar på att köpa tjänster bör ni undersöka om det finns säkerhetsbehov som ska tillgodoses genom åtgärder i er egen verksamhet. Finns det till exempel några behov som enklast löses med åtgärder i era egna IT-system, eller finns det beroenden av elektronisk kommunikation som är onödigt stora och går att minska?

För att bilda er en uppfattning om vad för tjänst ni bör köpa behöver ni ta reda på vad marknaden kan erbjuda och vilken risk, kostnad och funktion olika sorters lösningar kan innebära. Ni behöver slå fast vad som är viktigt för er och prioritera därefter. Ni bör också göra en bedömning av om det är några av era behov som kan vara extra kostsamma att uppfylla.

När ni formulerar krav på den tjänst ni ska köpa bör ni i första hand försöka beskriva vad ni vill uppnå och inte exakt hur det ska lösas. De krav som ställs ska vara mätbara så att det går att utvärdera olika lösningar och verifiera att kraven uppfylls över tid. Se till att det är tydligt hur avtalsuppföljning och incidenthantering ska hanteras av leverantören och er. Ni behöver också själva ha en förvaltning av de avtal som tecknas och följa upp hur era faktiska behov uppfylls över tid.

Tänk på att vissa risker i en elektronisk kommunikationstjänst behöver accepteras, medan andra risker kan vara oacceptabla för er verksamhet. Varje organisation bör ha en plan för att kunna upprätthålla kontinuiteten i sina allra viktigaste processer även om en stor incident inträffar. Om risken i verksamhetens elektroniska kommunikation bedöms vara oacceptabelt hög trots säkerhetsåtgärder bör kontinuitetsplanen omfatta reservlösningar som kan ersätta den elektroniska kommunikationen.

Kapitel 1

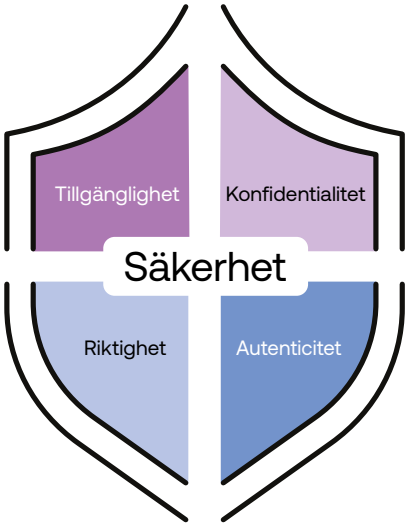
Vad är en säker elektronisk kommunikationstjänst?

I Lagen om elektronisk kommunikation (LEK) definieras säkerhet i nät och tjänster för elektronisk kommunikation så här: [1]

> *"...förmåga att vid en viss tillförlitlighetsnivå motstå händelser som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos näten eller tjänsterna, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster."*

En säker elektronisk kommunikationstjänst - kan sägas vara en tjänst som fungerar trots oönskade händelser.

Vi går på följande sidor igenom detta, alltså (1) vad det är som ska fungera, (2) vilka hoten och de oönskade händelserna kan vara och (3) hur säkerhet kan åstadkommas.



1 1 kap 7 § LEK

Vad är det som ska fungera?

Ur en användares perspektiv kan det som behöver skyddas i en tjänst beskrivas så här:

- **Tillgänglighet** – att kommunikationstjänsten är tillgänglig för användning, med de egenskaper som överenskommits
- **Konfidentialitet** – att informationen som överförs och uppgifterna om själva kommunikationen, till exempel vilka parter som kommunicerar, skyddas mot obehörig åtkomst.
- **Riktighet** – att informationen överförs utan att förvanskas.
- **Autenticitet** – att uppgifter om informationens ursprung, till exempel vilket telefonnummer som ringer, inte förvanskas utan är korrekta.

För att uppnå rätt nivå av säkerhet i de elektroniska kommunikationstjänster som er organisation använder behöver ni sätta dessa säkerhetsaspekter i relation till era behov. Här följer två korta exempel (i kapitel 3 beskriver vi hur ni kan gå till väga):

Exempel 1: Kommunikation av sjukvårdsjournaler. Att informationen är riktig, att obehöriga inte kan se den och att det går att lita på att den kommer från rätt källa är viktigt. Att kommunikationen kan vara otillgänglig en kortare tid kan däremot förmodligen accepteras.

Exempel 2: Kommunikation av trafiksignaler. Att informationen är riktig, att det går att lita på var den kommer från och att den är tillgänglig är viktigt. Att utomstående kan avlyssna informationen är förmodligen inte så allvarligt.

I exempel 1 är informationens konfidentialitet, riktighet och autenticitet viktig och behöver skyddas i hela kedjan. Genom att skydda dessa i organisationens egna system blir behoven av säkerhet i den kommunikationstjänst som används förmodligen mindre. Till exempel går det att öka skyddet för informationens konfidentialitet genom att informationen krypteras av organisationen själv innan den kommuniceras.

Det går alltså inte att sätta ett likhetstecken mellan organisationens behov av cybersäkerhet och kraven på säkerhet i de elektroniska kommunikationstjänster som organisationen köper. Av de fyra säkerhetsaspekterna för säker elektronisk kommunikation är tillgängligheten i många fall det som är svårast för organisationen att på egen hand säkerställa – om tjänsten är otillgänglig kommer kommunikationen inte att fungera oavsett vilka skyddsmekanismer användaren själv lägger till på tjänsten. Därför lägger vi extra vikt vid tillgänglighetsaspekten i denna vägledning.

Vilka är hoten mot elektronisk kommunikation?

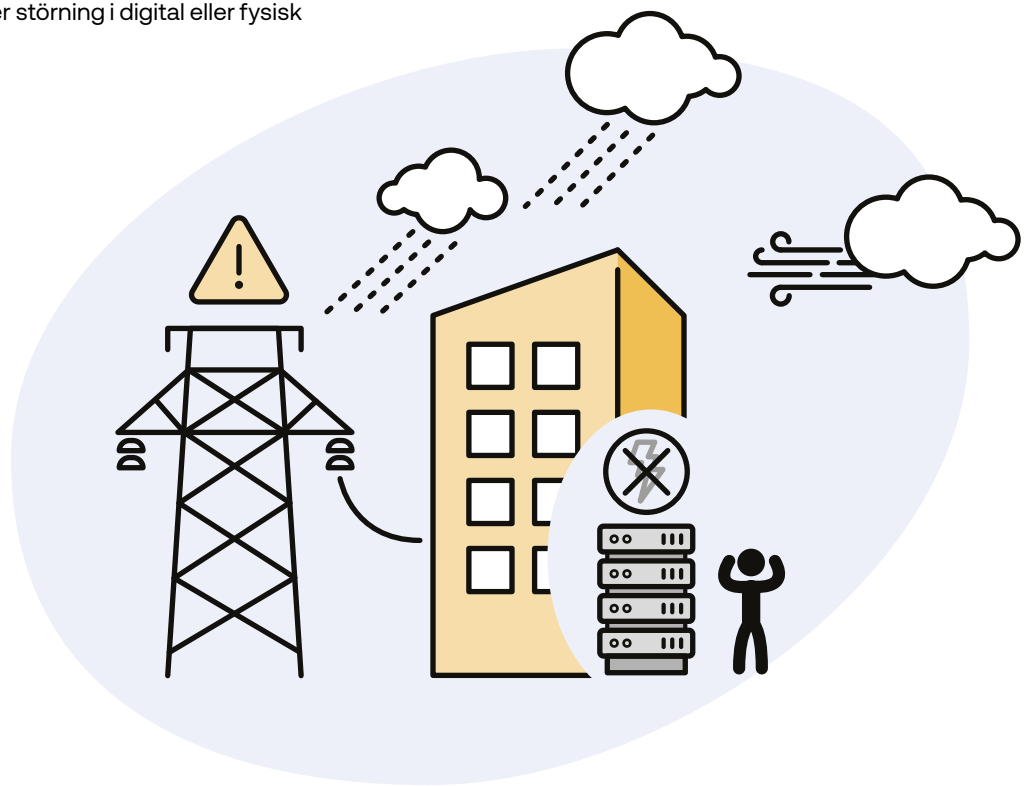
En säker elektronisk kommunikationstjänst ska fungera trots oönskade händelser. I detta avsnitt ska vi titta närmare på dessa händelser och vad som kan orsaka dem. Först ska vi introducera några viktiga begrepp:

- **Incident** – En oönskad händelse som ger en negativ inverkan på tillgängligheten, konfidentialiteten, riktigheten eller autenticiteten, eller på förmågan att motstå sådana händelser.
- **Hot** – Något som kan orsaka, eller bidra till att orsaka, en incident.
- **Risk** – En sammanvägning av sannolikheten att en oönskad händelse inträffar och konsekvenserna den i så fall får.
- **Sårbarhet** – Avsaknad av motståndskraft eller förberedelser som kan förhindra, eller bidra till att förhindra, en incident

För att elektronisk kommunikation ska fungera krävs en obruten kedja mellan avsändare och mottagare. Denna kedja byggs upp av elektronisk hårdvara, mjukvara, information, radioanvändning, samt kablar och annan fysisk infrastruktur - och den stöds av mänsklig aktivitet. Varje länk i kedjan behöver vara skyddad.

Hot mot elektronisk kommunikation kan till exempel komma från:

- **Fysisk påverkan från väder och omgivande miljö** – Nederbörd, is, hårda vindar, översvämning, fukt, vattenläckor, skred, skadliga temperaturer, skador orsakade av djur, brand, radiostörningar, solstormar, annan elektromagnetisk strålning, rymdkollisioner och förändringar av till exempel bebyggelse som hindrar radiosignaler.
- **Fel och brister i elnätet eller andra försörjningssystem** – Elavbrott, tekniska fel och brister i system för kraft eller inomhusklimat.
- **Fel och brister i hårdvara, mjukvara och information** – Tekniska fel och brister i elektronisk utrustning, kablar och andra fysiska komponenter. Buggar och sårbarheter i mjukvara, samt felaktig information.
- **Organisatoriska brister** – Otillräcklig försörjning av personal, kompetens, utrustning eller tredjepartstjänster. Bristfälliga processer inom incidenthantering, behörighetskontroll eller annat säkerhetsarbete.
- **Mänskliga misstag** – Felaktig hantering, konfigurationsfel, bristande segmentering av nätverk, fel vid uppdatering av mjukvara. Skadade kablar efter grävarbete, skador som orsakas vid snöröjning.
- **Antagonistisk påverkan** – Medvetet intrång, avlyssning, stöld, sabotage, förstörelse eller störning i digital eller fysisk infrastruktur.



Hur kan säkerhet åstadkommas?

De egenskaper som gör en tjänst säker – alltså som gör att den kan fungera trots oönskade händelser – kan delas in i två kategorier:

Robusthet – härdighet, en förmåga att stå emot påfrestningar.

Resiliens – förmåga till återhämtning och att klara av förändringa

Robusthet kan åstadkommas genom att skapa skyddsmekanismer och begränsa sårbara funktioner. Det kan till exempel göras med olika typer av fysiska skydd och kryptering av information. Resiliens kan åstadkommas genom att ha en design som är optimerad för snabb återstart och rutiner för att snabbt upptäcka och hantera avvikelser. Resiliens handlar också om att ha resurser, till exempel personal, reservdelar, säkerhetskopior och reservsystem, i beredskap.

Man kan förenklat säga att robusthet handlar om att härda ett system så att det blir så starkt att det kan stå emot oönskade händelser medan resiliens snarare handlar om att kunna hantera oönskade händelser när de ändå inträffar. Robusthet och resiliens är egenskaper som kompletterar varandra för att åstadkomma en samlad motståndskraft. För att undvika kostsamma lösningar som inte ger effekt är det viktigt att hitta rätt balans mellan robusthet och resiliens.

Två faktorer som är viktiga i designen för att åstadkomma säkerhet är redundans och diversitet:

Redundans – ett överskott av resurser.

Diversitet – mångfald, inbyggda olikheter.

Redundans innebär att det finns flera uppsättningar av en viss resurs, till exempel att det finns två system eller kablar i stället för bara en enda. Med redundans kan en funktion upprätthållas även om en enskild del slås ut, antingen direkt eller efter ett kortare avbrott. Diversitet innebär att det finns olikheter i systemet som gör att hela systemet inte är sårbart för samma sorts händelser. Diversitet kan vara fysisk (att resurser finns på skilda platser), teknisk (att olika tekniska lösningar används) eller organisatorisk (att flera olika leverantörer eller tillvägagångsätt används). Redundanta resurser är ofta diversifierade.

Hanterbar komplexitet - balanseras av struktur, kompetens och dokumentation.

Utöver redundans och diversitet finns det flera andra faktorer som också är viktiga för säkerheten, till exempel komplexitet. Ett system som har väldigt mycket redundans och diversitet men som saknar tillräcklig struktur kan till exempel bli så komplext att det snarare blir mindre robust och mindre resilient. Det är viktigt att komplexiteten i tekniska system och processer hålls på en hanterbar nivå och balanseras av struktur, kompetens och dokumentation.

Operatörer som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster i Sverige är skyldiga att följa de lagar och föreskrifter som reglerar säkerheten. Lag (2022:482) om elektronisk kommunikation (LEK) och Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2022:11) om säkerhet i nät och tjänster (PTS säkerhetsföreskrifter) ställer generella krav på operatörens säkerhetsarbete och specifika krav om till exempel redundans och diversitet i nät, system och elförsörjning som är viktiga för många användare. Utöver den grundnivå som krävs av lagar och föreskrifter har operatörerna också kommersiella drivkrafter för att upprätthålla säkerheten för sina kunder. I de följande kapitlen berättar vi mer om vad operatörerna konkret kan göra för att åstadkomma en viss säkerhet.

Det så kallade NIS2-direktivet [2] föreslås införlivas i svensk lag i början av 2025 genom en lag om cybersäkerhet. NIS2-direktivet innebär bland annat krav på anmälan, incidentrapportering och vidtagande av säkerhetsåtgärder (kallade riskhanteringsåtgärder enligt NIS2). Enligt nuvarande förslag till lag om cybersäkerhet kommer tillhandahållare av allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster att omfattas av kraven i den nya lagen. Vissa bestämmelser om säkerhet i nät och tjänster i LEK föreslås därmed att upphöra att gälla. NIS2-direktivet medför även att ytterligare sektorer kommer att omfattas av krav på riskhanteringsåtgärder, incidentrapportering och anmälan.

2 EU-parlamentets och rådets direktiv 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen

Kapitel 2

Så fungerar elektroniska kommunikationstjänster

För att kunna ställa relevanta krav på tjänster behöver ni som användare känna till några fundamentala begrepp och egenskaper i de nät och system som operatören producerar tjänster i. I det här kapitlet beskriver vi på en övergripande nivå hur dessa fungerar och belyser några aspekter som är relevanta för säkerheten.

Förr i tiden var nät och tjänster tätt integrerade system som var specialiserade för särskilda användningsområden. Till exempel fanns ett särskilt nät med inbyggda funktioner för telefoni, ett annat nät för kabel-tv, ytterligare ett nät för marksänd tv och så vidare.

Modern arkitektur för elektronisk kommunikation och digitala tjänster är modulär och i hög grad baserad på standarder. Nästan all kommunikation och alla typer av digitala tjänster bygger på att informationen som kommuniceras är förpackad i så kallade IP-paket. Det finns fortfarande flera olika nät, men de utför i princip alltid samma grundläggande uppgift: att transportera IP-paket. Ett nät används ofta till flera olika typer av tjänster.

Produktionen av de logiska funktioner – applikationer - som behövs för elektroniska kommunikationstjänster görs ofta på liknande sätt som för andra digitala tjänster, som till exempel webbapplikationer eller videoströmning. Applikationer produceras i mjukvara på till exempel applikationsservrar och i mobiltelefoner och använder information som lagras på databasservrar.

Den modulära arkitekturen i modern elektronisk kommunikation återspeglas också i leverantörskedjorna på marknaden. En operatörs nät och tjänster byggs i dag ofta upp av en blandning av infrastruktur, system, applikationer och tjänster som ägs och förvaltas av operatören själv, och delar som köps av andra operatörer och leverantörer. Operatörer säljer ofta tjänster i sitt nät på grossistbasis till andra operatörer. Sådana tjänster kan vara mer eller mindre förädlade, från till exempel fysiskt tillträde till fiberkablar, master och tekniklokaler till olika former av VPN-tjänster, internetanslutning, telefoni med mera.

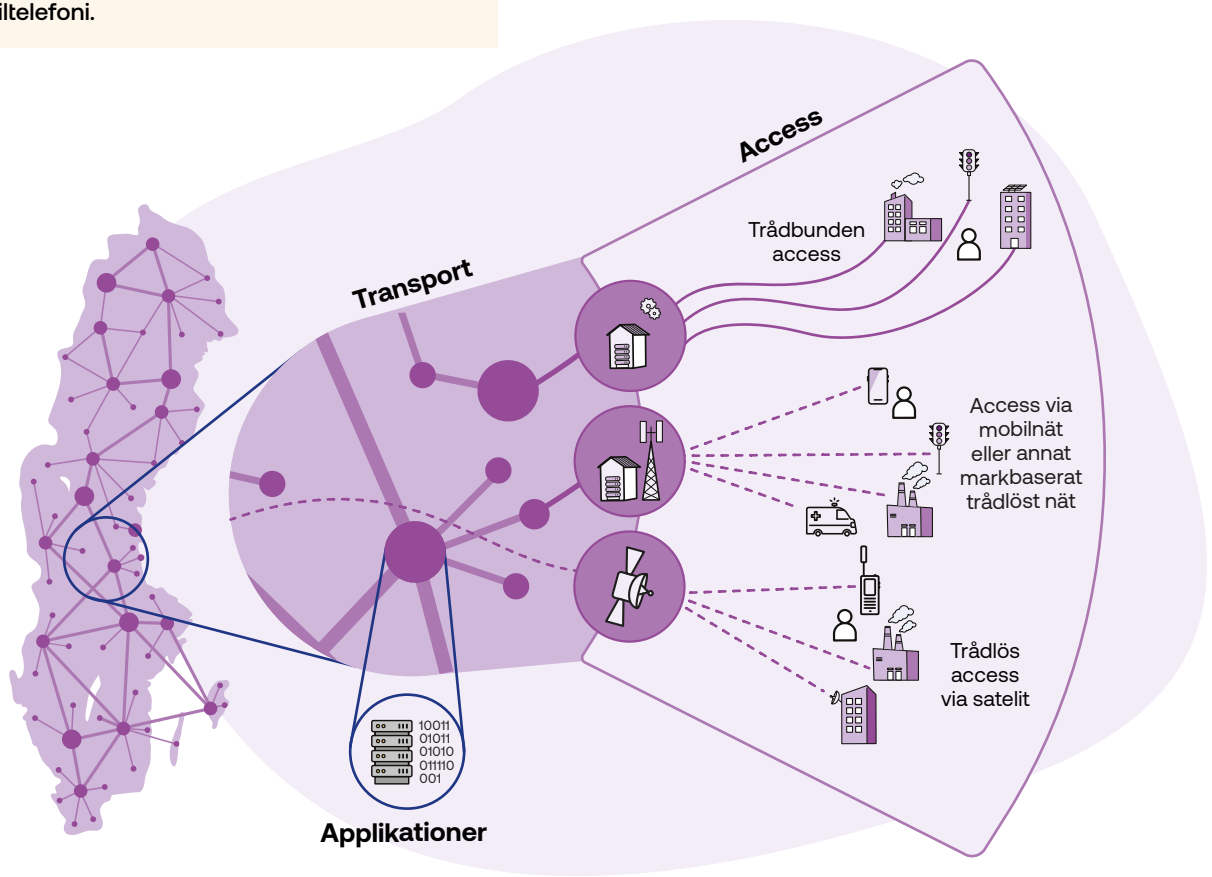
Tänk på:

Ett nät kan användas av flera olika operatörer och för flera olika typer av tjänster. Det innebär att du som användare behöver vara medveten om att det kan finnas gemensamma risker och sårbarheter även mellan två till synes helt olika tjänster som till exempel en fast internetanslutning och mobiltelefoni.

Produktionen av en elektronisk kommunikationstjänst kan förenklat brytas ned i följande tre delar:

- **Access** – Anslutning av en användare till ett nät, det som gör att användaren får tillgång.
- **Transport** – Förflyttning av information genom ett nät, det som gör att användare kan nå den eller det som användaren ska kommunicera med.
- **Applikationer** – De logiska funktioner och den data (information) som används till tjänster.

Här följer en beskrivning av hur dessa tre delar fungerar på en övergripande nivå.



Access – anslutning av en användare till ett nät

Access betyder att få tillgång till något. I det här sammanhanget är det en användare som får tillgång till en elektronisk kommunikationstjänst genom att ansluta till ett elektroniskt kommunikationsnät.

Den del av ett elektroniskt kommunikationsnät där användare ansluts kallas för accessnät. Det brukar definieras som den yttre del av nätet som sträcker sig från användaren till operatörens närmaste plats med teknisk utrustning. Utrustningen på denna plats sköter kommunikationen med användare i ett visst område och hanterar transport vidare in i nätet. Lokalen där utrustningen finns tillgodoser utrustningens behov av el, klimatkontroll och skydd.

Användarens access är antingen trådbunden eller trådlös. En trådbunden access är alltid fast installerad och alltså bunden till en specifik plats medan en trådlös access kan vara såväl fast installerad (platsbunden) som mobil (rörlig). En fast installerad mobilnätsrouter är ett exempel på fast trådlös access.

Med en trådbunden access ansluts användare via kablar som innehåller trådar av optisk fiber eller koppar, som bär lasersignaler eller elektriska signaler. Kablarna är förlagda under marken eller hänger i stolpar längs med gator och vägar. Med jämna mellanrum finns nedgrävda brunnar eller små skåp så att underhållspersonal kommer åt kablarna. På de flesta platser i Sverige där människor bor och verkar varaktigt finns ett eller flera trådbundna accessnät.

I ett mobilnät ansluts användare trådlöst via radiosignaler i ett radioaccessnät, användarna delar på en viss mängd radiospektrum (alltså ett utrymme för radiosignaler). I de svenska mobilnäten finns flera olika typer av mobilnätsteknik, dels de äldre generationerna 2G och 3G som är under avveckling, dels de mer moderna 4G och 5G. Det finns också tekniker i mobilnäten som är utformade för att ansluta strömsnåla sensorer och liknande som inte behöver överföra så mycket information. På de flesta platser i Sverige där människor bor och verkar varaktigt finns flera olika mobilnät. Utöver de nationella mobilnäten förekommer flera andra typer av markbaserade trådlösa accessnät, både allmänt tillgängliga och privata.

Tänk på:

Robustheten och resiliensen i ett allmänt elektroniskt kommunikationsnät är ofta som lägst i accessnätet eftersom det är förhållandevis få användare som är beroende av det.

Det bör inte förutsättas att det finns redundans och diversitet i nät och elförsörjning för en trådbunden access om inte användaren ställt specifika krav på sin tjänst.

Trådlösa signaler exponeras för omgivningen på ett helt annat sätt än trådbundna signaler. Tillgängligheten kan hotas medvetet eller omedvetet av annan radioanvändning, väderfenomen och omgivande miljö. Att själva radiosignalen är mer lättåtkomlig för utomstående innebär också vissa risker för konfidentialitet, riktighet och autenticitet i överföringen av information.

Användning av radiosändare kräver tillstånd från PTS, förutom för vissa användningar som är undantagna från tillståndsplikt. De nationella mobilnäten använder tillståndspliktigt radiospektrum. Användningar som inte kräver tillstånd delar ofta frekvensband med andra användningar vilket kan innebära större risker för radiostörningar eller kapacitetsbrist som kan påverka tillgängligheten.

För mobilnätens radioaccessnät finns krav [3] på att de ska vara försedda med viss reservkraft för att kunna stå emot kortare elavbrott, se avsnittet ”Motståndskraft mot elavbrott” i kapitel 5.

För att en trådlös access ska fungera krävs att det finns en god radiotäckning på den plats där den ska användas.

3 11 kap. 10 § PTS Säkerhetsföreskrifter

I satellitkommunikationsnätverk ansluts användare trådlöst via radiosignaler till en satellit i rymden. Satelliten är i sin tur ansluten till ett transportnät genom en trådlös anslutning till en så kallad markstation eller en annan satellit. På grund av de stora avstånden ger satellitnät radiotäckning till mycket stora områden på jorden. Av samma anledning har satellitnät en större tidsfördröjning i signalöverföringen och lägre överföringskapacitet per användare än vad markbaserade elektroniska kommunikationsnät generellt sett har. Det finns flera satellitkommunikationsnät med täckning i Sverige.

Vilken typ av utrustning som används för att ansluta användaren till ett nät varierar, bland annat beroende på vad det är för sorts tjänst och access. Det kan till exempel vara en router, en switch, en mobiltelefon, en dator eller en satellitterminal. I den här vägledningen använder vi begreppet användarutrustning för att beskriva den utrustning som är användarens gränssnitt till operatörens nät. Fast installerad användarutrustning benämns ofta CPE, Customer Premises Equipment.

Tänk på:

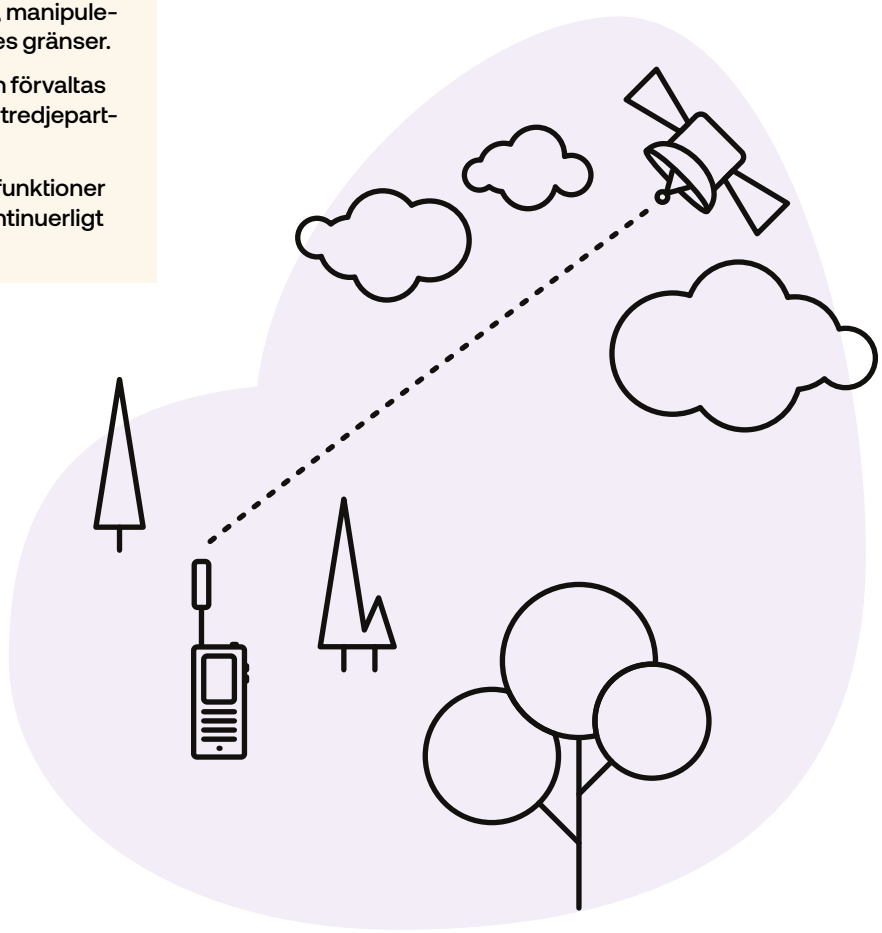
Själva satelliterna har egen strömförsörjning som inte är beroende av det svenska elnätet.

En satellitaccess kan i vissa fall vara helt oberoende av annan elektronisk kommunikation eller elnät i Sverige.

Satellitkommunikationsnätverk sträcker sig utanför Sveriges gränser och tillhandahålls ofta av operatörer från andra länder. Det innebär en lägre nivå av svensk kontroll och att signaler kan nås och potentiellt störas, manipuleras eller avlyssnas från platser utanför Sveriges gränser.

Användarutrustningen kan tillhandahållas och förvaltas av operatören, av användaren själv eller av en tredjepartsleverantör.

Användarutrustningen innehåller ofta viktiga funktioner såsom en brandvägg. Det är viktigt att den kontinuerligt hålls uppdaterad.



Transport – förflyttning av information genom ett nät

Transport handlar om att flytta något från en plats till en annan. I det här sammanhanget är det information, oftast förpackad i så kallade IP-paket och märkta med mottagarens IP-adress, som transporteras i form av signaler genom elektroniska kommunikationsnät.

Den del av ett elektroniskt kommunikationsnät som utför denna transport kallas för transportnät och det kan förbinda stadsdelar, städer, regioner och länder. Transportnätet ansluter till accessnäten och binder på så sätt samman användare på olika platser. Till transportnätet är också operatörens applikationer anslutna, alltså de servrar där funktioner för olika elektroniska kommunikationstjänster tillhandahålls.

Transportnäten är ofta trådbundna med kablar av optisk fiber, särskilt de stora transportstråken som bär stora mängder trafik långa sträckor. Trådlös anslutning via radio används också, till exempel vid anslutning av satelliter och i vissa fall vid anslutning av basstationer för mobiltelefoni. På platser där olika stråk i nätet möts finns utrustning som hanterar signalöverföringen och dirigerar trafiken. I utkanten av transportnätet kan det handla om switchar som samlar upp trafik från många små stråk, medan det i knutpunkterna inne i nätet är routrar som dirigerar IP-paket åt rätt håll genom att titta på paketets adressat och jämföra med sitt adressregister.

Tänk på:

Eftersom transportnät spänner över stora avstånd och innehåller mängder av teknik går det inte att helt undvika fel. Kablarna i näten kan också vara förlagda på platser som gör det svårt att snabbt reparera fel, till exempel under vatten, i en högspänningsledning eller i direkt närhet till en stor väg eller järnväg. Därför är redundans och diversitet i både kablar, teknisk utrustning och elförsörjning viktigt för att upprätthålla tillgängligheten. Större transportstråk är ofta mer robusta än de mindre.

Mängden trafik som transporteras i ett nät varierar över tid, det kan uppstå situationer då efterfrågan överstiger nätets kapacitet. En operatör kan under vissa förutsättningar särbehandla trafik för att säkra en viss överföringskvalitet för en tjänst även när nätet är överbelastat. Det kan till exempel användas för telefoni som är känslig för fördröjningar.

Olika operatörers nät ansluter till varandra för att användare ska kunna nå andra användare, information och digitala tjänster som finns i andra operatörers nät. Det sker på olika sätt beroende på ändamål och bygger på överenskommelser mellan operatörer.

Internet är en infrastruktur med många sammankopplade nät som var för sig administreras självständigt, men som tillsammans bildar en global infrastruktur. Näten tillhör olika operatörer och andra aktörer som exempelvis stora leverantörer av digitala tjänster, företag, myndigheter och organisationer. Genom att varje nät utbyter IP-trafik och routinginformation (vilka adresser som kan nås genom nätet) med ett eller flera andra nät möjliggörs i förlängningen en global transport av IP-paket. Internet betraktas som publikt eftersom alla får ansluta sig till det och det inte kontrolleras av någon enskild aktör.

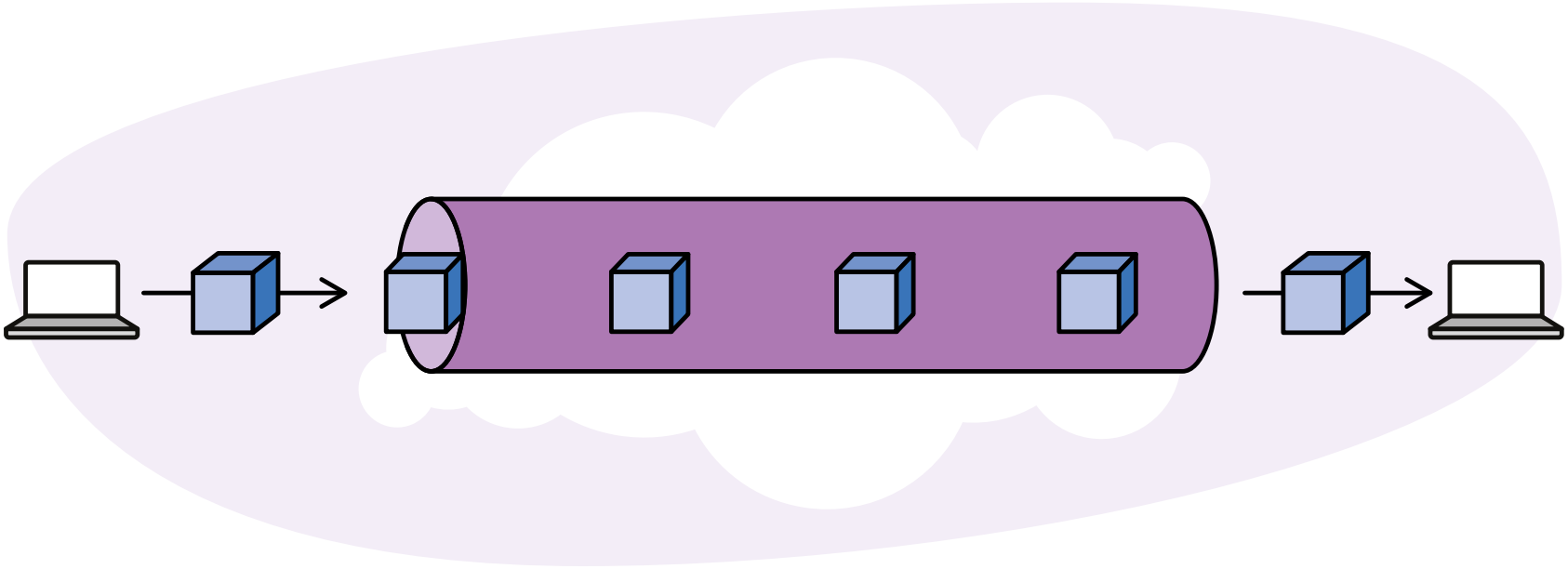
Tänk på:

Transport över publika nät så som internet medför vissa säkerhetsrisker. I många fall behöver konfidentialitet, riktighet och autenticitet skyddas genom att använda kryptering och andra skyddsmekanismer.

Internet som helhet har en hög redundans och diversitet vilket gör det till en resilient infrastruktur för transport. Ingen enskild aktör kan dock garantera att information som transporteras över internet når fram, det brukar benämnas som ”best effort”. Trafik på internet får enligt EU-förordningen om öppet internet [4] inte diskrimineras. Det innebär bland annat att en viss användares trafik inte får prioriteras framför andra.

Utbyte av routinginformation mellan olika operatörer på internet görs oftast med routingprotokollet Border Gateway Protocol, BGP. Det är baserat på tillit mellan de operatörer som utbyter routinginformation, vilket gör det sårbart både för avsiktliga attacker och felkonfigurationer. Det kan till exempel vara kapning av trafik, förvanskning av IP-adresser och att trafik dirigeras fel av misstag. Felaktig routinginformation kan ge kaskadeffekter och spridas över internet. För att upprätthålla säkerheten behöver säkerhetsåtgärder vidtas av operatören, till exempel övervakning för att kunna upptäcka och åtgärda avvikelser.

4 EU förordning 2015/2120 om åtgärder rörande en öppen internetanslutning



Ett privat nät är inte tillgängligt för allmänheten. Med privata nät kan viss trafik, till exempel för olika användare eller olika sorters tjänster, separeras. Att skapa privata nät med fysisk separation över långa sträckor är kostsamt, det vanligaste är att i stället göra det virtuellt med logisk separation. Det finns flera olika tekniker för att skapa virtuella nät. Det görs typiskt genom att förpacka trafiken eller på annat sätt märka trafiken med en etikett som visar att den ska dirigeras en viss väg eller hanteras på ett visst sätt. Ett virtuellt privat nät, ett VPN, bygger på så kallade tunnlar där trafik förpackas vid tunnelns ingång och packas upp vid tunnelns utgång. Med hjälp av kryptering kan konfidentialiteten för innehåll, avsändare och adressat skyddas. För att skydda riktighet och autenticitet kan signering och kontrollfunktioner också användas.

Tänk på:

Ett så kallat ändpunktsbaserat VPN skapas med funktionalitet som finns i till exempel användarutrustningen eller i användarens eget system. Ett sådant VPN kan skapas av användaren själv och spänna över flera olika underliggande nät.

Ett så kallat nätbaserat VPN skapas av operatören med funktionalitet i den tekniska utrustningen inne i operatörens nät. Det kan möjliggöra en ökad kontroll av hur trafiken transporteras, till exempel kan operatören i vissa fall avsätta en viss överföringskapacitet för en särskild användare. Det är en åtgärd för tillgänglighet, men ska i normalfall inte behövas så länge nätet är dimensionerat i förhållande till efterfrågan.

Applikationer – logiska funktioner som används till tjänster

Produktionen av en elektronisk kommunikationstjänst görs förutom i själva nätet även i mjukvarufunktioner, applikationer, som ofta finns på applikationsservrar.

Vissa av dessa applikationer är synliga för användaren och vissa används av utrustningen inne i operatörens nät och syns inte för användaren. Applikationer används till allt från att dela ut IP-adresser och autentisera användare till att koppla upp telefonsamtal, hantera meddelanden och alla andra funktioner i de elektroniska kommunikationstjänster vi använder. Applikationerna är beroende av information om till exempel telefonnummer och adresser som typiskt lagras på databasservrar.

Servrar med applikationer och information finns på olika platser. De är ofta distribuerade (det vill säga utspridda på flera platser), till exempel i datorhallar (datacenter) och molnlösningar runt om i Sverige och i världen. Vissa tillhandahålls av operatören själv, andra finns hos operatörens underleverantörer och andra aktörer.

Information som används för att producera en tjänst kan befinna sig i tre olika stadier – i vila, under bearbetning och i rörelse. Informationen kan hanteras av många olika aktörer på flera olika platser och behöver hållas säker i alla dessa led vilket kan vara en komplex utmaning för operatören.

Om vi tar ett telefonsamtal som exempel behövs det information om vem som initierar samtalet och vem som ska ta emot det. I vila kan informationen vara säkrad i en databasserver. När samtalet kopplas upp sätts informationen i rörelse och skickas till en applikationsserver för att bearbetas. Informationen har då passerat tre olika stadier. Informationen kan ha gått via flera olika nät och hamnat i applikationsservar hos partnerorganisationer, både i Sverige och utomlands.

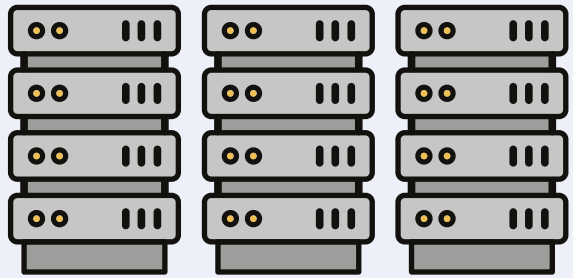
Komplexiteten varierar mellan olika elektroniska kommunikationstjänster. En vanlig telefonitjänst kan till exempel vara mindre komplex än en tjänst som också har växel- eller kontaktcenterfunktionalitet. En tjänst med trådlös access via mobilnätet är beroende av applikationer och information i nätet för att hantera mobilitet och radiogränssnitt som inte behövs i en motsvarande tjänst med trådbunden access.

Tänk på:

Att applikationer och information är säkra är en mycket viktig del av säkerheten för en elektronisk kommunikationstjänst i stort. Fel i mjukvara och servrar är till exempel några av de vanligare orsakerna till stora incidenter. Antagonistiska cyberangrepp är också ett stort hot mot säkerheten.

Det är svårt att som användare få insyn i och kunna bedöma specifika delar av operatörens cybersäkerhetsarbete. Framför allt handlar det om att operatören behöver bedriva ett systematiskt säkerhetsarbete, det skriver vi mer om i kapitel 5.

Komplexitet kan medföra större risker. För vissa behov kan det därför finnas anledning att välja enklare lösningar.



Kapitel 3

Kartlägg användningen av elektroniska kommunikationstjänster och behovet av säkerhet i organisationen

För att kunna tillgodose organisationens behov av säkra elektroniska kommunikationstjänster behöver ni först bilda er en tydlig uppfattning av vad det är organisationen behöver. Ett första steg är att kartlägga vilka av era verksamhetsprocesser som behöver elektroniska kommunikationstjänster och vilka säkerhetsaspekter som är viktiga för dessa processer. Hur omfattande kartläggningen blir beror på vad det är för verksamhet och vilken kunskap och dokumentation ni redan har. Involvera de delar av organisationen som behövs för att få en tydlig bild.

Organisationens användning av elektroniska kommunikationstjänster

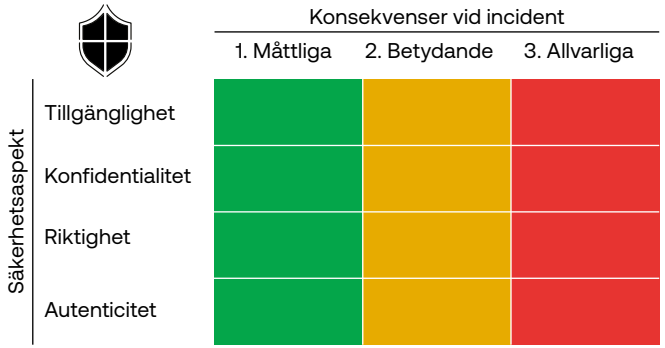
I det första steget behöver ni kartlägga vilka elektroniska kommunikationstjänster som organisationen behöver och för vilka processer. Kartläggningsbehovet kan vara sprunget ur att organisationen avser att gå ut i en ny upphandling av elektroniska kommunikationstjänster eller att någon process i verksamheten ska förändras.

Kartläggningen bör åtminstone beskriva det följande för respektive process:

- Vad processen syftar till
- På vilken eller vilka platser den utförs
- Vem eller vad som det behöver kommuniceras med
- Vilken typ av kommunikation som behövs, till exempel telefoni eller datakommunikation
- Vilka nuvarande elektroniska kommunikationstjänster som används

Bedöm organisationens säkerhetsbehov

Nästa steg i kartläggningen är att identifiera vilka säkerhetsaspekter som är relevanta och bedöma konsekvenserna för organisationen om säkerheten inte upprätthålls. Vilka säkerhetsaspekter som är viktiga och hur viktiga de är varierar sannolikt mellan organisationens olika processer. Till exempel kan det för vissa processer vara mycket viktigt med konfidentialitet medan tillgänglighet är av mindre vikt, för andra processer kan situationen vara den omvända. Ett mycket användbart verktyg är klassningsmodellen från informationssakerhet.se[5]. En enkel modell kan ställas upp så här:



För att bedöma konsekvenserna bör ni beskriva vad är det som konkret skulle hända om säkerheten i en process inte kan upprätthållas vid en incident i den elektroniska kommunikationen. Det kan till exempel vara:

- Ekonomiska konsekvenser, direkta och indirekta
- Minskat förtroende för er organisation
- Rättsliga konsekvenser, till exempel att inte kunna leva upp till lagar eller avtal med kunder
- Konsekvenser för samhällets funktionalitet och dess skyddsvärden

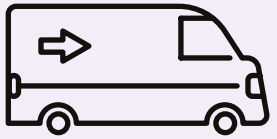
Gör också en bedömning av om, och i så fall på vilket sätt konsekvenserna varierar beroende på omfattning, tidpunkt och varaktighet av en incident. Till exempel:

- Hur lång tid behöver incidenten vara innan den negativa konsekvensen uppstår?
- Blir konsekvenserna större om incidenten inträffar en viss tid på dygnet, veckan eller året?
- Hur påverkas konsekvenserna av återkommande incidenter över tid?

Försök att beskriva konsekvenserna på ett sätt som gör det möjligt att sätta dem i relation till kostnaden för säkerhet.

5 https://www.informationssakerhet.se/siteassets/metodstod-for-lis/1.-om-metodstodet/vagledning-utforma-klassningsmodell_kommentarsperiod.pdf

Exempel

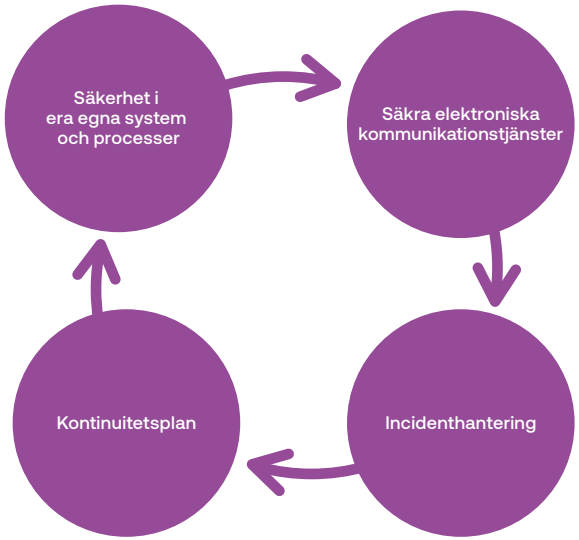


	Exempel 1: Kommunikationen till butikens digitala betalsystem	**Exempel 2: Digitalisering av handläggning av marktillstånd**	**Exempel 3: Telefoni för organisationens fältservicepersonal**
Process	Ta betalt	Kommunens handläggning av marktillstånd	Fältservice
Utförs på plats	Butiken, Långgatan 3	Kontoret, Storgatan 1	Mobilt, på vägarna i hela Sverige
Kommunikation med	Bankens it-system	Remissinstanser och ansökanden	Kunder och kollegor
Kommunikation via	Internet	I dagsläget fysiska brev	Telefoni
Nuvarande kommunikationslösning	Bankens VPN via butikens mobila bredband	Ingen elektronisk kommunikation i dagsläget	Mobilabonnemang
Tillgänglighet	Avbrott längre än en vardag eller fyra timmar under helgen får betydande ekonomiska konsekvenser. Fler än tre–fyra sådana avbrott per år får allvarliga konsekvenser. Avbrott längre än två timmar under december får allvarliga ekonomiska konsekvenser.	Om det inträffar fler än två–tre dygnslånga avbrott per månad får det betydande konsekvenser för verksamheten. Avbrott på helger ger ingen påverkan.	Att telefonin för enskilda servicetekniker då och då inte fungerar i upp till en arbetsdag får bara måttliga konsekvenser. Avbrott som drabbar samtliga servicetekniker i en region kan få betydande konsekvenser. Återkommande otillgänglighet, till exempel dålig radiotäckning vid en större andel av kundernas adresser, kan få allvarliga konsekvenser.
Konfidentialitet	Information innehåller personuppgifter som om de röjs kan ge betydande förtroendemässiga och rättsliga konsekvenser.	Om information som är belagd med sekretess röjs kan det få betydande konsekvenser, framför allt rättsliga och förtroendemässiga.	Röjande av information som kommuniceras via telefon bedöms endast få måttliga konsekvenser.
Riktighet	Om informationen inte är korrekt kan det ge betydande ekonomiska konsekvenser.	Om informationen som ligger till grund för beslut och senare tillämpning inte är korrekt kan det få allvarliga konsekvenser, såväl rättsliga som förtroendemässiga och ekonomiska.	Om informationen som kommuniceras via telefon inte är korrekt ger det endast måttliga konsekvenser.
Autenticitet	Om uppgifterna om informationens ursprung inte är korrekt kan det få betydande ekonomiska konsekvenser.	Om uppgifterna om informationens ursprung inte är korrekt kan det få allvarliga konsekvenser, såväl rättsliga som förtroendemässiga och ekonomiska.	Om uppgifterna om informationens ursprung inte är korrekt, till exempel att det uppringande telefonnumret är förfalskat, skulle det bara ge måttliga konsekvenser.

Kapitel 4

Ta fram en plan för att uppfylla ert behov av säkerhet

När ni har en tydlig bild över hur elektroniska kommunikationstjänster används i era processer och vilka säkerhetsaspekter som är viktiga så kan ni ta fram en plan för hur behoven ska tillgodoses. Målet är att identifiera hur ni bäst kan lösa organisationens säkerhetsbehov. Det innebär att ni behöver jämföra olika alternativ och hitta en lösning med en acceptabel risk och kostnad. Det handlar både om att undersöka vilken säkerhet som finns, eller bör finnas, i organisationens egna system och processer, och vilken säkerhet som krävs i de elektroniska kommunikationstjänster som köps in. Det handlar också om att bedöma vilka risker som ni måste acceptera och att vidta åtgärder för att säkra kontinuitet i de viktigaste delarna av er verksamhet även vid stora incidenter. Det är inte en linjär process, ni kan till exempel behöva gå tillbaka och titta på alternativa lösningar i era processer och system om önskad säkerhet inte går att uppnå i en viss elektronisk kommunikationstjänst.



Säkerhet i organisationens egna system och processer

Innan ni ställer krav på säkerheten i de elektroniska kommunikationstjänster som organisationen behöver bör ni undersöka vilka säkerhetsbehov som ska tillgodoses i organisationens egna system och processer.

Säkerhet i form av konfidentialitet, riktighet och autenticitet för datakommunikation mellan två system kan ofta åstadkommas genom åtgärder i systemen i fråga, till exempel behörighets- och åtkomstregler i systemen samt kryptering av kommunikation till och från systemen. Tillgängligheten i den elektroniska kommunikationen är ofta den säkerhetsaspekt som är svårast för organisationen att påverka i de egna systemen.

Det kan också finnas processer där nyttan av elektronisk kommunikation inte väger upp kostnaden för säkerhet och där beroendet av elektroniska kommunikationer bör reduceras. Det kan till exempel gälla ett system som egentligen skulle fungera bra utan uppkoppling, men som idag är konfigurerat så att det kräver internetuppkoppling för att fungera. Eller ett system som bara kräver uppkoppling för att en leverantör ska kunna konfigurera det på distans, och där effektivitetsvinsten är lägre än kostnaden för att uppnå tillräcklig säkerhet i den elektroniska kommunikationen.

Vilken säkerhet som krävs i organisationens elektroniska kommunikationstjänster påverkas också av var organisationens egna applikationer och information finns i förhållande till den plats de ska nås från. Det kan finnas anledning att se över vad som lagras i molnet eller annan distribuerad lagring och vad som lagras lokalt på till exempel kontoret. Om lagring sker lokalt på samma plats som informationen eller applikationen ska användas på krävs inte en elektronisk kommunikationstjänst för att nå den. Distribuerad lagring kan å andra sidan ge bättre förutsättningar för redundans i kommunikationen än vad som går att uppnå med lagring på en enskild plats.

Ett exempel: Om organisationen har applikationer och information som alltid ska vara tillgängliga för användare via internet, till exempel en e-tjänst eller webbsajt, kan det i vissa fall vara mer effektivt att placera dessa i molnet eller annan lösning för distribuerad lagring än att försöka uppnå motsvarande säkerhet i internetanslutningen till en server på kontoret. Om organisationen å andra sidan har digitala resurser som alltid måste vara tillgängliga, men bara från kontoret, kan behovet av säkerhet i den elektroniska kommunikationen reduceras om de lagras på kontoret i stället för i molnet.

För att organisationens processer ska vara säkra gäller det att hela kedjan är säker. Utöver att se till att de elektroniska kommunikationstjänster som ni köper är säkra behöver ni också se till säkerheten i de delar av er elektroniska kommunikationslösning som ni själva förvaltar. Det kan till exempel handla om ert lokala nätverk eller den användarutrustning som används till den köpta elektroniska kommunikationstjänsten. Om detta inte ingår i operatörens ansvar är det viktigt att ni själva kan förvalta och hålla detta säkert.

Sammanfattning:

- ✓ **Undersök vilken säkerhet som ska tillgodoses i organisationens egna system och processer.**
- ✓ **Se över om det finns onödiga beroenden av elektronisk kommunikation.**
- ✓ **Var organisationens digitala resurser är placerade påverkar behoven av säker elektronisk kommunikation.**
- ✓ **Glöm inte att det ni själva förvaltar också måste vara säkert, till exempel ert lokala nätverk eller användarutrustning.**

Exempel 1: **Kommunikation till butikens betalsystem**

Behoven av säkerhet är stora ur alla aspekter . Men tillräcklig konfidentialitet, riktighet och autenticitet säkerställs i detta exempel av banken genom säkerhetsåtgärder i bankens betalterminal, bankens it-system och i det VPN som använder butikens internetanslutning.

Exempel 2: **Digitalisering av handläggning av marktillstånd**

Behoven av säkerhet är stora för konfidentialitet, riktighet och autenticitet. I detta exempel kan organisationen sannolikt själv implementera tillräckliga säkerhetsåtgärder för konfidentialitet, riktighet och autenticitet. När informationen är i vila behöver den skyddas genom behörighets- och åtkomstregler i organisationens it-system. När informationen distribueras kan den skyddas med en krypteringslösning mellan organisationens system.

Elektroniska kommunikations-tjänster som tillgodoser era behov

Efter att ni har kartlagt vilka säkerhetsaspekter i en elektronisk kommunikationstjänst som är viktiga för er behöver ni undersöka hur de kan tillgodoses av marknaden, och vilka krav som är viktiga att få med i ett inköp eller en upphandling.

Ett första steg kan vara att titta på vilka olika typer av elektroniska kommunikationstjänster som kan vara relevanta. För att få en bild av vilka lösningar som finns kan ni studera operatörernas produktinformation och rådgöra med experter inom området eller personer inom ert nätverk som har liknande behov i sin verksamhet.

Det är i detta skede också önskvärt att kunna påbörja en dialog med olika operatörer för att utforska vilka sorters lösningar som finns på marknaden. Observera att det är mycket viktigt att organisationens inköps- eller upphandlingsfunktion driver denna process så att formkraven följs. För offentliga organisationer finns bestämmelser i upphandlingslagstiftning som behöver följas. Det är viktigt att inte ge vissa leverantörer konkurrensfördelar genom att ge dem förhandsinformation om era behov eller kommande krav. Det finns sätt att få svar på frågor utan att ge en viss leverantör en konkurrensfördel, till exempel en Request for Information (RFI) som riktas till alla tänkbara leverantörer. En RFI görs innan upphandlingen inleds, som en del av marknadsanalys och behovsinventering. Upphandlingslagstiftningen medger i vissa fall också både förhandling och dialog under själva upphandlingsprocessen.

Exempel på frågor som kan vara lämpliga att lyfta i ett tidigt skede är:

- Vilka typer av tjänster och lösningar finns det och vilka kan vara lämpliga?
- Hur har detta lösts för andra liknande organisationer? Finns det goda exempel och potentiella fallgropar?
- Hur sannolikt är det att relevanta säkerhetsaspekter kan upprätthållas med olika lösningar?
- Finns det delar som är svåra att lösa eller som är särskilt kostnadsdrivande, till exempel vissa typer av säkerhetslösningar eller anslutning i vissa områden?

Ni måste själva bedöma hur djupt ni behöver gå i förberedande dialog och analys innan ni har bildat er en uppfattning om vad ni vill köpa och kan formulera det i en kravställning. Vi ger en fördjupning av kravställning och inköp i kapitel 5.

Sammanfattning:

- ✓ **Undersök hur ert säkerhetsbehov kan tillgodoses av marknaden, och vilka krav som är viktiga att få med i ett inköp eller en upphandling**
- ✓ **För att få en bild av vilka lösningar som finns kan ni granska operatörernas produktinformation och rådfråga experter eller liknande organisationer.**
- ✓ **Det är i detta skede också önskvärt att kunna påbörja en dialog med olika operatörer för att utforska vilka sorters lösningar som finns på marknaden, men se till att inköps- eller upphandlingsorganisationen leder processen.**

Exempel

Vi återbesöker de tre exemplen som vi följt och visar ett förenklat resonemang. I dessa är det tillgängligheten som är den viktigaste säkerhetsaspekten i de elektroniska kommunikationstjänsterna. Vilka typer av tjänster skulle kunna lösa behoven? Och kan tillräcklig säkerhet erbjudas till en acceptabel kostnad och med rimliga villkor?

Exempel 1: Kommunikation till butikens betalsystem.

Organisationen har bedömt att avbrott längre än en vardag eller fyra timmar under helger får betydande konsekvenser. Fler än 3–4 sådana avbrott per år eller enskilda avbrott överstigande två timmar under december bedöms ge allvarliga konsekvenser.

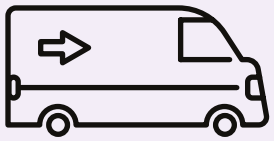
De bedömer att det finns goda möjligheter att köpa en tjänst som sannolikt (men inte garanterat) kommer att tillgodose behovet av hög tillgänglighet, men till en relativt hög kostnad.

I detta läge kan de göra en bedömning av risk för olika alternativ genom att väga samman konsekvensen med sannolikheten. I exemplet bedömer de att den bästa avvägningen mellan risk och kostnad är att ställa krav på en maximal återställningstid vid avbrott på fyra timmar och att själva implementera en lösning för offline-betalning för att kraftigt reducera konsekvenserna av avbrott under julhandeln.

Exempel 2: Digitalisering av handläggning av marktillstånd.

Organisationen har bedömt att fler än 2–3 dygnslånga avbrott per månad skulle ge betydande konsekvenser. De bedömer att sannolikheten är mycket låg för avbrott i den omfattningen, även om inga krav ställs på tillgängligheten utöver vad som erbjuds som standard på marknaden.

I exemplet gör de därför bedömningen att den bästa avvägningen mellan risk och kostnad är att kraven på tillgängliga ska vara måttliga och i linje med standard.



Exempel 3: Telefoni för organisationens fältservicepersonal.

Organisationen har bedömt att avbrott som drabbar samtliga servicetekniker i en region skulle ge betydande konsekvenser. Återkommande otillgänglighet, till exempel dålig täckning vid en större andel av kundernas adresser, bedöms kunna ge allvarliga konsekvenser. Avbrott som kan drabba alla operatörens abonnenter i en region är ovanliga, men det kan inte uteslutas att det kan inträffa några gånger per år.

Eftersom sådana avbrott skulle ge betydande negativa konsekvenser för er gör de i exemplet bedömningen att organisationens inköp av mobilabonnemang bör fördelas mellan två olika operatörer, alternativt att vissa av serviceteknikerna ska få tillgång till två mobilabonnemang.

De undersöker möjligheterna att ställa krav som gör att eventuella gemensamma sårbarheter hos operatörerna begränsas. Samtidiga avbrott i flera olika mobilnät bedöms som mindre sannolika. Eftersom dålig radiotäckning på platser där serviceteknikerna behöver arbeta bedöms kunna ge allvarliga konsekvenser kommer krav på täckning att ställas och kontrolleras. Flera operatörer bedöms ha nät med god täckning där det behövs.

Beredskap att hantera incidenter

Oavsett hur säker en lösning är kommer det alltid att inträffa incidenter. Det är viktigt att ha förmågan att hantera dessa.

Att skapa en förmåga att hantera incidenter inom elektronisk kommunikation är i grunden inte skilt från organisationens allmänna incidenthanteringsförmåga. Det finns flera rapporter och webbplatser som ger vägledning inom incidenthantering, några finns samlade som lästips sist i denna vägledning.

Det handlar till stor del om att ha rätt organisation, kompetens och rutiner på plats och att ha planerat och övat i förväg hur problem ska hanteras, både inom organisationen och tillsammans med leverantörer. Hur ansvarsfördelning och samarbete mellan operatör och användarorganisation ska se ut behöver vara tydligt överenskommet i förväg.

Några saker som är viktiga att tänka på när det gäller att hantera incidenter i de elektroniska kommunikationstjänster som organisationen använder är:

- Hur gör ni för att upptäcka olika typer av incidenter?
- Hur kan operatören upptäcka och informera om incidenter?
- Hur eskaleras incidenter i operatörens organisation?
- Hur kan ni bedöma om orsaken till incidenten finns i den elektroniska kommunikationstjänsten eller i era egna system?
- Kan operatören bistå med incidenthantering även om det inte är säkert att orsaken finns i den elektroniska kommunikationstjänsten?
- Hur informerar operatören om status på en felavhjälpning?
- Hur kan operatören medverka i att utreda vad som orsakat incidenter, finns spårbarhet?

Sammanfattning:

- ✓ **Skapa rutiner för hur incidenter ska hanteras.**
- ✓ **Se till att ansvarsfördelning, rapportering och kontaktvägar mellan er och operatören är tydliga.**

Kontinuitet för organisationens viktigaste processer även vid stora incidenter

Varje organisation bör ha en plan för att kunna upprätthålla kontinuiteten i de allra viktigaste processerna, trots stora incidenter. Vi ger i detta avsnitt några exempel på detta. Myndigheten för samhällsskydd och beredskap (MSB) har ett mer omfattande material om kontinuitetsplanering, se lästipsen i slutet av denna vägledning.

Om risken bedöms vara oacceptabelt hög trots de säkerhetsåtgärder som kan vidtas i organisationens ordinarie elektroniska kommunikationstjänst bör kontinuitetsplanen omfatta reservlösningar för elektronisk kommunikation. Om ni kartlagt organisationens behov av elektronisk kommunikation, identifierat och värderat risker och vidtagit åtgärder för säkerhet har ni redan kommit en bra bit på vägen.

Att ta fram en kravbild för reservlösningar för elektronisk kommunikation bygger i grund och botten på samma principer som för att göra organisationens ordinarie kommunikationslösning säkrare. För att reservlösningen verkligen ska fungera när det gäller bör det säkerställas att de beroenden, hot eller sårbarheter som motiverar lösningen undviks. En viktig skillnad jämfört med organisationens ordinarie lösning för elektronisk kommunikation är att reservlösningen bara behöver klara av de allra viktigaste tillämpningarna. Reservlösningen behöver inte hålla samma prestanda och kvalitet utan bara tillräckligt för det som är viktigast. Om er verksamhet klarar sig med en reservlösning eller om det krävs flera alternativa reservlösningar för att hantera samma risk beror på hur viktigt det är att verksamheten kan upprätthållas. Glöm inte att reservlösningen behöver testas och övas på.

Exempel på hur elektroniska kommunikationstjänster kan användas som reservlösning:

- En tjänst hos en annan operatör än ordinarie operatör
- En trådlös anslutning via satellit eller mobilnät som reserv till en trådbunden anslutning och tvärtom
- Telefoniabonnemang som fungerar oberoende av er ordinarie växel, eller en alternativ telefonväxel som reserv till er ordinarie

Exempel på hur förändrad användning av den elektronisk kommunikationen kan fungera som reservlösning:

- Att kunna använda chatt och röstkommunikation via internet i stället för telefoni
- Att kunna logga in i verksamhetssystem med tvåfaktorsautentisering via internet i stället för via sms
- Att kunna klara sig trots kraftigt nedsatt prestanda
- Att kunna ringa med mobiltelefonen via wifi i stället för via mobilnätets radioaccessnät

Tänk på att en reservlösning även kan behöva hantera störningar hos eller i den elektroniska kommunikationen till era leverantörer och andra tredjepartsaktörer, till exempel:

- Att kunder ska kunna logga in i era tjänster även om det saknas fungerande kommunikation till den vanliga e-legitimationsleverantören
- Att ni ska kunna ta emot betalningar även om det saknas fungerande kommunikation till den vanliga betaltjänstleverantören
- Att det finns en reservversion av er webbsajt eller digitala tjänst hos en annan leverantör

Organisationen kan också behöva ha en reservlösning för hur de allra mest kritiska processerna ska kunna upprätthållas även i ett läge då de elektroniska kommunikationerna inte fungerar. Till exempel:

- Att ha beredskap för att hantera arbetsuppgifter manuellt, till exempel att hemtjänstverksamheten kan göra hembesök om trygghetslarm och telefoni inte fungerar, eller att kunna öppna kontorets dörrar och garageportar med en fysisk nyckel om fjärruppkopplingen inte fungerar.
- Att kunna använda digitala system offline. Till exempel att ha en lokal kopia av den information som behövs för organisationens allra viktigaste uppgifter eller att kunna logga in i eventuella lokala verksamhetssystem med tvåfaktorsautentisering utan att använda internet eller sms. Eller att som butiksverksamhet kunna ta emot kortbetalningar offline, eller andra betalningsmedel som fungerar utan elektronisk kommunikation.

Sammanfattning:

- ✓ **Organisationen bör ha en plan för hur kontinuitet i de viktigaste processerna ska säkerställas vid större incidenter.**
- ✓ **Reservlösningar när det gäller elektronisk kommunikation kan handla om användning av en annan tjänst, förändrad användning av befintlig elektronisk kommunikation, och beredskap för att kunna upprätthålla de allra mest kritiska processerna även om ingen elektronisk kommunikation fungerar.**

Kapitel 5

Att utforma kravställning och köpa säkra elektroniska kommunikationstjänster

När ni har bildat er en uppfattning om era behov kan ni utforma er kravställning och genomföra ett inköp.

I detta kapitel ger vi först en introduktion till kravställning och därefter ger vi ett antal exempel på hur några vanligt förekommande säkerhetsbehov kan lösas. Dessa exempel syftar framför allt till att ge er en insikt om faktorer som påverkar säkerheten, och olika åtgärder som en operatör kan vidta för att möta säkerhetskraven. Tillsammans med de föregående kapitlen i denna vägledning kan exemplen hjälpa er att identifiera era funktionsmässiga behov, ställa rätt frågor till operatörer och utvärdera olika lösningar. Exemplen kan också användas som utgångspunkt för mer specifika krav. Exemplen är inte heltäckande och de är inte ett facit för er specifika verksamhet. Vi har också samlat några lästips i form av rapporter och webbsajter som kan vara till hjälp på de sista sidorna av denna vägledning.

Förutom er inköps- eller upphandlingsfunktion bör representanter för verksamheten som ska använda tjänsten och eventuellt även experter inom till exempel teknik också delta i arbetet. Som nämnts i föregående kapitel är det mycket viktigt att organisationens inköps- eller upphandlingsfunktion driver denna process så att formkraven för själva processen kan följas. Vi går i denna vägledning inte närmare in på hur själva inköps- eller upphandlingsprocessen går till utan det är upp till er organisation.

Att ställa krav i en inköpsprocess

I processen att utforma krav är det viktigt att förstå och kunna formulera organisationens behov och sätta sig in i vad marknaden kan erbjuda. Inom offentlig upphandling måste ni förhålla er till den så kallade proportionalitetsprincipen som innebär att krav måste stå i proportion till era behov. Vid offentlig upphandling får kraven alltså inte vara hårdare än vad som behövs. Motivera de krav ni ställer utifrån era behov. För att hitta rätt balans mellan risk och kostnad är det viktigt att förstå vad en operatör kan och inte kan påverka och vad som är särskilt kostnadsdrivande. Ni kan behöva prioritera mellan vilken säkerhet som ska uppnås genom robusthet respektive resiliens, mellan säkerhet i en ordinarie lösning respektive en reservlösning och mellan vad verksamheten ska lösa själva respektive köpa som tjänst. Tänk också på att det inte behöver vara exakt samma lösning till allt och på alla platser.

I utformningen av krav bör fokus ligga på vad ni vill uppnå och inte hur det ska lösas. Sträva efter att formulera krav på funktion och undvika att detaljstyra hur den ska åstadkommas. I första hand bör kravställningen för tjänstens säkerhet utgå från organisationens identifierade behov av säkerhet för de fyra aspekterna tillgänglighet, konfidentialitet, riktighet och autenticitet. Detsamma gäller för de behov organisationen har identifierat i övrigt - ställ i första hand krav på funktionalitet som till exempel mobilitet snarare än att ställa krav på en specifik teknik eller accesstyp om det inte är nödvändigt. Genom att ställa krav på funktion snarare än att detaljstyra kan onödiga begränsningar och fallgropar undvikas.

Det betyder inte att kravställningen ska vara svepande och övergripande. Har ni identifierat särskilda behov av funktioner eller risker och hot som är specifika för er organisation bör dessa omsättas till krav som då kan vara relativt specifika. Det kan till exempel handla om att er organisation identifierat en risk för sabotage som gör att det finns behov av ett specifikt skydd. Eller att organisationen lyder under viss lagstiftning eller andra krav på verksamheten som behöver omsättas i specifika krav på tjänsten. Det kan också handla om sådant som är specifikt för den plats där er verksamhet bedrivs, till exempel att det är en förhöjd risk för översvämning eller skred eller att det pågår omfattande ombyggnationer i ert närområde som gör att säkerheten behöver vara starkare än annars.

Det finns också situationer då det kan behövas relativt detaljerade tekniska krav, till exempel för att säkra kompatibilitet mellan olika tekniska system. I de fall ni köper en tjänst som ska bäras av era andra tjänster, till exempel att ni köper telefoni som ska bäras av er internetanslutning, behöver ni kontrollera vilka krav som måste ställas på tjänsterna för att det ska fungera. Sådana krav bör så långt som möjligt knytas till etablerade standarder.

Ni bör också försäkra er om att själva tjänsten ni köper kommer att fortsätta tillhandahållas över en tillräcklig tid. Detta är särskilt viktigt för tillämpningar där det är kostsamt att göra ändringar, till exempel uppkopplade prylar på otillgängliga platser. Hur etablerad är tekniken och hur länge kommer operatören att stödja den? Ett exempel är den pågående avvecklingen av 2G- och 3G-näten.

Sammanfattning:

- ✓ **För att hitta rätt balans mellan risk och kostnad är det viktigt att kunna beskriva organisationens prioriterade behov och förstå vad som är särskilt kostnadsdrivande**
- ✓ **När ni formulerar krav, fokusera på funktion och inte tekniken bakom.**

Glöm inte uppföljning

Alla krav bör vara mätbara, så det går att utvärdera olika lösningar och verifiera att kraven uppfylls över tid. Många operatörer erbjuder analysverktyg för att följa upp och verifiera kvaliteten på leveransen, det kan ingå i kravställningen av tjänsten. Det finns också andra metoder för uppföljning så som uppföljningsmöten eller olika typer av stickprovstester.

En plan för avtalsuppföljning bör tas fram i samband med inköpet. Av planen ska det framgå hur avvikelser hanteras, samt hur eskalering ska göras. Det är viktigt att hitta en rimlig riskfördelning mellan kund och leverantör när det kommer till avvikelser. Ett avtal kan innehålla klausuler om vite eller skadestånd vid avvikelser, ni behöver själva bedöma vad som är lämpligt. Det bör också vara tydligt vad som krävs för att avtalet ska kunna sägas upp. Tänk på att det är viktigt att ta hänsyn till vilka faktorer som operatören kan påverka och vilka som är svårare att kontrollera. Krav på skadestånd eller viten för faktorer som operatörer har svårt att påverka kan leda till ett försämrat utbud och högre kostnader, utan att tjänsten i sig blir bättre.

Ni behöver själva ha en förvaltning av de avtal som tecknas. Det är inte bara kraven ni ställde vid köptillfället som behöver följas upp, utan även hur era faktiska behov uppfylls över tid. Det innebär att ni kontinuerligt behöver ha en god bild av vilka era behov är och att ni också kan behöva göra justeringar i lösningen. Justeringar kan till exempel behöva göras vid förändringar i hotbild, teknikutveckling, förändrade regelverk och lagar eller vid förändringar i er verksamhet. Över tid kan det också framkomma delar som ni missat i kravställningen, till exempel säsongsrelaterade utmaningar eller om andra negativa konsekvenser identifieras med tiden. Tänk på att det vid offentlig upphandling finns begränsningar av hur ett avtal får justeras utan att genomföra en ny upphandling.[6]

Sammanfattning:

- ✓ **Se till att kraven är mätbara.**
- ✓ **När ni ska komma fram till en rimlig riskfördelning mellan er och leverantören är det viktigt att förstå vad som ligger inom operatörens kontroll och vad som inte gör det.**
- ✓ **Ta fram en plan för hur avtal ska följas upp.**
- ✓ **Följ upp hur era faktiska behov uppfylls över tid, de kan förändras.**

6 17 kap. 8-14 §§ Lagen om offentlig upphandling

Operatörens generella säkerhetsarbete

Operatörens generella arbete med säkerhet är mycket viktigt för säkerheten i de tjänster som operatören tillhandahåller. Utöver de krav som ställs på säkerheten för en specifik tjänst kan det, beroende på era behov, vara relevant att ställa krav på det generella säkerhetsarbetet hos den operatör som tillhandahåller tjänsten.

LEK och PTS säkerhetsföreskrifter ställer grundläggande krav på att operatörer ska bedriva ett långsiktigt, kontinuerligt och systematiskt säkerhetsarbete [7]. PTS säkerhetsföreskrifter ställer bland annat följande krav på operatörer: [8]

- Det ska finnas tydliga och väl dokumenterade rollfördelningar med utpekade ansvariga för säkerhetsarbetet. System och processer ska vara dokumenterade och det ska säkerställas att personalen förstår och tar del av dokumentationen.
- Det ska finnas system för hantering och kontroll av identiteter och behörigheter, både för operatörens personal och dess uppdragstagare.
- Åtkomst till system och tillgångar ska loggas och nät och tjänster ska kontinuerligt övervakas. Det ska finnas larmsystem för störningar och avbrott. Incidenter ska kunna hanteras dygnet runt.

PTS:s säkerhetsföreskrifter ställer också krav på operatörers riskhantering, bland annat följande: [9]

- Riskanalys ska göras regelbundet och vid förändringar, till exempel vid uppdatering av system och när hot förändras. Beslut om riskhantering ska dokumenteras.
- Åtgärder för att undvika eller reducera risker ska vara anpassade till den risk som föreligger, med beaktande av kostnader och vilken teknik som finns tillgänglig.
- Risker bör endast accepteras om säkerheten i nät och tjänster i stort kan upprätthållas även om hotet förverkligas eller incidenten inträffar.

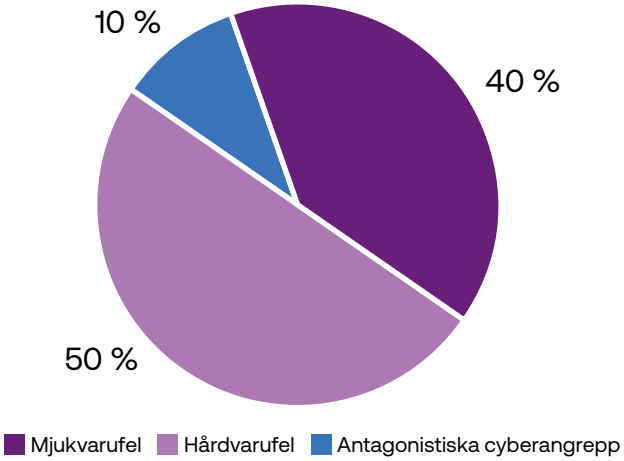
7 8 kap 1 § LEK samt 3-17 kap PTS Säkerhetsföreskrifter

8 3, 4, 7, 9 och 12 kap PTS Säkerhetsföreskrifter

9 5 och 6 kap PTS Säkerhetsföreskrifter

Trots förebyggande åtgärder inträffar incidenter. Säkerhetsincidenter som har haft en betydande påverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten i nät och tjänster ska rapporteras av operatören till PTS. Mindre incidenter rapporteras inte in till PTS.

Inrapporterade incidenter med betydande påverkan på säkerheten 2022-2023



Under 2022–2023 rapporterades knappt 70 incidenter med betydande påverkan på säkerheten till PTS.

Drygt 40 procent av incidenterna orsakades av olika former av mjukvarufel, mestadels beroende på buggar i mjukvara eller felaktigt utförda konfigurationsarbeten i mjukvara, och mänskliga misstag. Att ha bra processer för att hantera förändringar i nät och tjänster är en viktig förutsättning för att motverka incidenter av denna typ och att snabbare kunna åtgärda de som ändå inträffar. Det kan till exempel handla om hur mjukvaruuppdateringar testas innan de installeras och hur snabbt kan man reagera och dra tillbaka en felaktig uppdatering.

Hälften av incidenterna orsakades av elavbrott och olika former av hårdvarufel, mestadels i servrar och nätverksutrustning som exempelvis routrar. Fungerande redundans och reservkraft är viktiga förutsättningar för att förhindra denna typ av incidenter.

Återstående knappt 10 procent av incidenterna orsakades av antagonistiska cyberangrepp, varav hälften i form av logiska överbelastningsangrepp och hälften i form av intrång i operatörens system. Cybersäkerheten hos operatören och dess underleverantörer är kritisk för säkerheten. Moderna it-system och rutiner för att snabbt åtgärda nya sårbarheter är exempel på hur operatörer kan skydda sina nät mot intrång och attacker. Se även de rapporter och webbsajter vi listat under lästips sista i denna vägledning.

Ledningssystem som till exempel ISO 27000 (ledningssystem för informationssäkerhet) kan kan ge en vägledning om aspekter av operatörens generella säkerhetsarbete som kan vara relevanta att ställa krav på. Observera att det inom offentlig upphandling inte anses proportionerligt att ställa uttryckliga krav på certifiering enligt till exempel ISO. En certifiering kan användas som bevis på att operatören uppfyller en viss nivå, men inte vara ett krav i sig. I vissa fall kan det också vara relevant att ställa frågor eller krav på specifika områden som till exempel operatörens leveranskedja, i sådana fall rekommenderar vi att ni tar hjälp av experter som kan göra en oberoende bedömning av riskerna.

Sammanfattning:

- ✓ **Operatörens generella arbete med säkerhet är mycket viktigt för säkerheten i de tjänster som operatören tillhandahåller.**
- ✓ **Utöver de krav som ställs på säkerheten för en specifik tjänst kan det även vara relevant att ställa krav på organisation och säkerhetsarbete hos den operatör som tillhandahåller tjänsten.**
- ✓ **Dessa aspekter är oftast inte är något som en operatör förändrar på beställning, utan det handlar snarare om att välja rätt operatör i förhållande till era behov**

Avtalad tillgänglighet

Tillgänglighet är ett av de vanligaste säkerhetskraven som användare ställer på sin operatör. Det kallas ibland för ”service-nivå” eller ”service availability” och betyder helt enkelt tillgång till tjänsten.

Krav på tillgänglighet formuleras vanligtvis med följande parametrar:

- Tillgänglighet – I vilken omfattning, beräknat över en viss tidsperiod, ska tjänsten vara tillgänglig med de egenskaper som avtalats, det vill säga felfri?
- Fel – Vad räknas som ett fel på tjänsten och vad är bara nedsatt funktion?
- Felanmälan – Under vilka tider kan fel anmälas och hur ska det göras?
- Inställelsetid – Hur lång tid får det ta innan arbetet för att åtgärda ett fel påbörjas?
- Åtgärdstid – Hur lång tid får det ta att återställa tjänstens tillgänglighet?
- Servicefönster – Med vilka villkor, hur ofta och under vilka tider får planerade avbrott i tjänsten göras för operatörens underhållsarbete?

För den grundläggande tillgänglighet som ofta erbjuds som standard finns det som regel inga garantier, utan avbrott ska anmälas och operatören åtar sig att åtgärda avbrottet så fort som möjligt. När en specifik tillgänglighet avtalas beskrivs den ofta som en procentandel av tid. För att bedöma vilken tillgänglighet som din verksamhet behöver kan det hjälpa att räkna om den till hur stor del av tiden som tjänsten maximalt får vara otillgänglig. En tjänst med 99 procent tillgänglighet dygnet runt får till exempel vara otillgänglig i sammanlagt drygt tre och ett halvt dygn per år. Sätt er in i det finstilta – viktiga begrepp som tillgänglighet och åtgärdstid kan beräknas på olika sätt och det är viktigt att ni förstår vad ni köper, så ni kan se om det uppfyller era behov.

Det är också viktigt att förstå att en avtalad tillgänglighet inte är ett facit på hur tjänsten faktiskt kommer att fungera i framtiden. I bästa fall är det en trovärdig bild av vad som kan förväntas baserad på en väl grundad bedömning av risker, sårbarheter och förmågan att hantera dessa hos operatören. Där behovet av tillgänglighet är stort är det viktigt att ni sätter er in i tjänstens egenskaper och hur operatören ska uppfylla tillgängligheten, för att kunna bedöma trovärdigheten i operatörens åtagande.

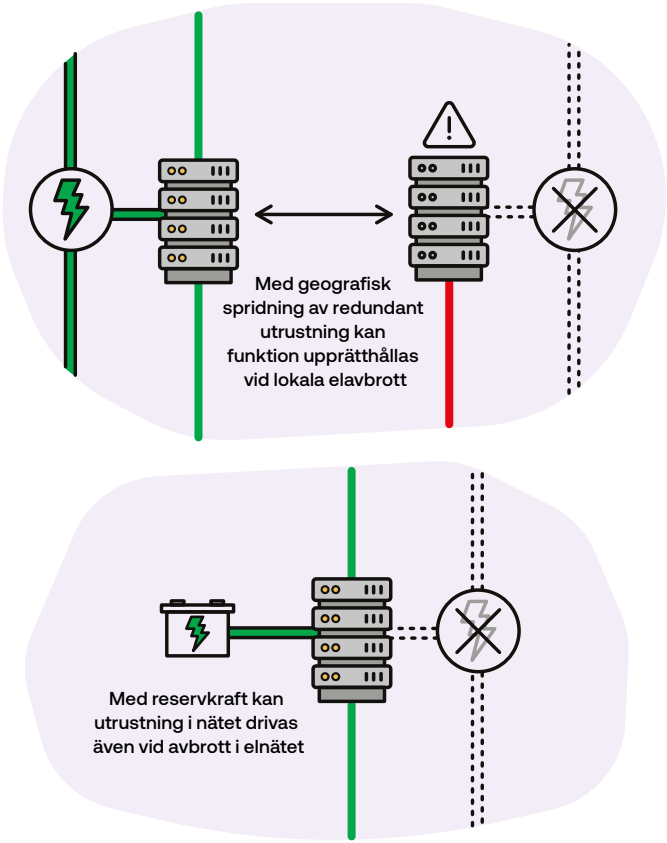
Som tidigare nämnts är det viktigt att förstå vilka faktorer som operatören kan påverka. En operatör kan till exempel aldrig förutse hur lång tid det tar att avhjälpa alla typer av fel, men kan sannolikt i hög grad kontrollera hur lång tid det får ta innan arbete för att åtgärda felet inleds. Tillgängligheten kan också stärkas av lösningar för robusthet som till exempel redundans, diversitet och reservkraft. Även åtgärder för resiliens som övervakning av tjänstens funktionalitet, lagerhållning av reservdelar och beredskap i serviceorganisationen är handfasta saker som kan öka möjligheten att upprätthålla en hög tillgänglighet. Vilken tillgänglighet som kan erbjudas och till vilken kostnad varierar, bland annat mellan olika platser och mellan olika accessformer.

Det kan vara svårare att bedöma grundorsaken till avbrott i tillgänglighet för en trådlös anslutning än för en trådbunden anslutning. En trådlös anslutning kan bara upprätthållas om användaren befinner sig inom radiotäckningen. Om tillgängligheten plötsligt upphör där det brukar finnas täckning är det uppenbart att det handlar om ett avbrott. Men om användaren rör sig i områden utan täckning kan inte denna företeelse betraktas som ett fel på tjänsten om inte det har avtalats om att en viss täckning ska finnas. Det är därför viktigt att användaren kontrollerar täckningen i det relevanta området. Mobiloperatörernas täckningskartor kan ge en viss vägledning, liksom PTS information och vägledning för en bättre mobiltäckning [10]. Om det är särskilt viktigt rekommenderas en oberoende mätning.

10 www.pts.se/tackning

Sammanfattning:

- ✓ **Se till att det är tydligt vad som räknas som fel på tjänsten, hur fel ska hanteras och i vilken omfattning tjänsten ska vara tillgänglig och fri från fel.**
- ✓ **En avtalad servicenivå är inte ett facit.**
- ✓ **Konkreta säkerhetsåtgärder som till exempel redundans, diversitet, reservkraft, övervakning och beredskap för serviceorganisationen kan förstärka tillgängligheten.**
- ✓ **För en trådlös anslutning är det viktigt att kontrollera att det finns radiotäckning där tjänsten ska användas.**



Motståndskraft mot elavbrott

All elektronisk kommunikation är beroende av el. Om det inte finns en inbyggd motståndskraft för att kunna stå emot elavbrott räcker det med ett avbrott någonstans i kedjan för att kommunikationen ska brytas.

Enligt Energimarknadsinspektionen var det under 2022 [11] i genomsnitt 76 minuters elavbrott per elabonnent. Det finns relativt stora geografiska skillnader, på landsbygden är elavbrott generellt mer frekventa och mer långvariga än i tätorter. Knappt 50 000 elabonnenter drabbades av elavbrott som varade längre än 12 timmar och drygt 8 000 drabbades av elavbrott längre än 24 timmar.

Elektroniska kommunikationsnät kan göras motståndskraftiga mot elavbrott genom att bygga in redundans och diversitet både i själva nätet och dess elförsörjning. Med redundanta och geografiskt spridda (diversifierade) uppsättningar av utrustning i nätet kan nätet motstå elavbrott som inte drabbar flera platser samtidigt. Reservkraft i form av batterier eller dieselgeneratorer kan användas som redundans till ordinarie elförsörjning via elnätet. Storleken på batterierna eller mängden bränsle i tanken styr hur långa elavbrott som kan motstås.

Vilken motståndskraft som finns mot elavbrott varierar mellan olika nät, tjänster, operatörer och platser. PTS:s säkerhetsföreskrifter ställer vissa grundläggande krav på både reservkraft, redundans och diversitet i näten, baserade på hur konsekvenserna vid avbrott ser ut.[12]

För funktioner i näten som många användare är beroende av finns krav på reservkraft för att kunna stå emot elavbrott. Reservkraften ska i de fallen räcka för drift i mellan 2 och 24 timmar, beroende på antal användare.[13] För mobilnät finns krav på reservkraft även för funktioner i näten som få användare är beroende av, vilket inkluderar radioaccessnätet. Reservkraften ska räcka för drift av nätet i minst en timme i tätort och minst fyra timmar utanför tätort.[14] Satelliter producerar sin egen el, så satellitkommunikationsnät har en inbyggd motståndskraft mot elavbrott på jorden, förutsatt att berörda delar av nätet på jorden har el.

Om organisationens elektroniska kommunikationstjänst måste kunna motstå elavbrott med en viss varaktighet är det viktigt att ställa krav på detta. För en trådbunden access kan operatörer erbjuda en anpassning så att den är försörjd med reservkraft med en viss uthållighet. I praktiken kan det innebära att koppla ett batteri till användarutrustningen, samt att koppla användarens accessnätsanslutning till en av operatörens tekniklokaler som har reservkraft, förbi eventuella platser längs vägen som inte har reservkraft.

Tänk på att många användare saknar reservkraft på sina tjänster med trådbunden access. Vid ett elavbrott kan det därför bli en hög belastning på mobilnäten när många användare vill använda det i stället för trådbundna nät.

MSB tillhandahåller elektroniska kommunikationstjänster, som till exempel radiokommunikationstjänsten Rakel, till vissa tillämpningar hos behöriga samhällsviktiga organisationer. Rakel används till exempel av polis, räddningstjänst och vissa myndigheter och kan drivas med reservkraft en längre tid. Du kan läsa om detta på MSB:s webbsajt.

Även satellitkommunikationstjänster kan i många fall erbjudas med hög motståndskraft mot elavbrott.

Ska ni bedriva verksamhet vid elavbrott är det viktigt att ni också säkrar reservkraft för användarutrustning samt de övriga system och elektroniska utrustning som ska användas. Mobiltelefoner, satellittelefoner och annan användarutrustning för mobilt bruk har egna batterier. Det är viktigt att regelbundet underhålla reservkraft i form av batterier eller dieselgeneratorer för att den ska fungera när det behövs.

Sammanfattning:

- ✓ **Om organisationens elektroniska kommunikationstjänst måste kunna motstå elavbrott med en viss varaktighet är det viktigt att ställa krav på detta.**
- ✓ **Operatörer är skyldiga att ha reservkraft på vissa viktiga funktioner som många användare är beroende av. Hur länge den ska kunna drivas vid ett elavbrott beror på antalet användare.**
- ✓ **För trådbundna accesser saknas ofta reservkraft om inte användaren specifikt ställt krav på det. För mobilnätens radioaccessnät finns krav på reservkraft som räcker för drift i minst en till fyra timmar, beroende på geografi. Satellitkommunikationstjänster kan ha en hög motståndskraft mot elavbrott.**
- ✓ **Ska ni bedriva verksamhet vid elavbrott är det viktigt att ni också säkrar reservkraft för de övriga system och elektroniska utrustning som ska användas.**

11 ei.se/bransch/eloverforingens-kvalitet/leveranssakerhet-i-elnatet

12 11 kap PTS Säkerhetsföreskrifter

13 11 kap 1, 2 och 8 §§ PTS Säkerhetsföreskrifter

14 11 kap 10 § PTS Säkerhetsföreskrifter

Redundans och diversitet

Redundans innebär att bygga in ett överskott med flera uppsättningar av viktiga resurser och funktioner, så att tjänsten kan upprätthållas även vid fel på enstaka delar. Diversitet innebär att bygga in olikheter så att en enskild händelse inte leder till fel på flera delar samtidigt. Vilken redundans och diversitet som redan finns inbyggd i operatörens nät och tjänster varierar. PTS:s säkerhetsföreskrifter ställer vissa grundläggande krav på redundans och diversitet i näten, i relation till hur många användare som är beroende av en viss funktion.[15] De stråk och funktioner i näten som är viktiga för många användare är ofta byggda med redundans och geografisk diversitet.

Redundans och diversitet kan i vissa fall utökas på begäran av en användare för att möta högre krav på säkerheten i en tjänst. Det är inte troligt att en operatör kan bygga om de centrala delarna av sitt nät för en enstaka användare, men det kan vara möjligt att stärka användarens access och välja en alternativ implementation av tjänsten som ger en högre redundans och diversitet. Förutsättningarna kan variera avsevärt mellan olika platser och operatörer. Det finns ofta goda förutsättningar att åstadkomma redundans och diversitet för en tjänsts access i tätbefolkade områden, medan det i mer glesbefolkade områden ofta är svårare eftersom infrastrukturen där typiskt sett är glesare.

För en trådlös access kan det finnas en viss grundläggande diversitet, i det fall det finns flera basstationer med täckning i området. För en trådbunden access krävs generellt att användaren aktivt ställer krav för att tjänsten ska förses med redundans och diversitet. Att åstadkomma fysisk diversitet för en trådbunden access kräver inte sällan att nätet byggs om, vilket kan vara kostsamt. Figuren nedan visar några alternativ för redundans och diversitet i accessnät.

En operatör kan också erbjuda redundans och diversitet i accessen genom att kombinera en trådbunden och en trådlös access, till exempel via mobilnätet. Det kan ofta göras utan att nätet behöver byggas om. För en sådan lösning är det viktigt att tänka på att överföringskapaciteten vanligtvis är lägre i trådlösa nät och normalt inte kan garanteras. Tänk också på att det inte är självklart att en trådlös och en trådbunden förbindelse är separerade i transportnätet.

15 11 kap 1-7 §§ PTS Säkerhetsföreskrifter

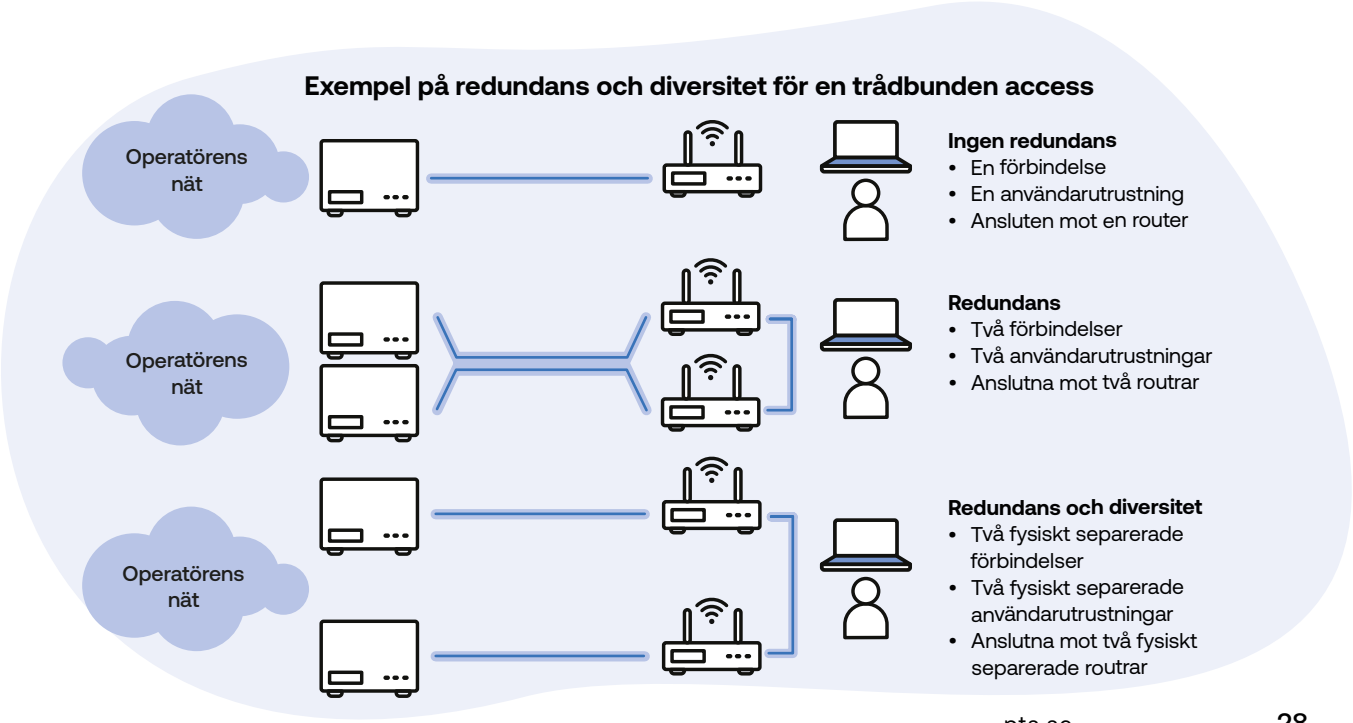
Om organisationens krav på säkerhet är höga kan redundans och diversitet behövas. Det är dock viktigt att ta hänsyn till att operatörens bedömning av vad som krävs för att uppnå en viss säkerhet bygger på en bedömning av sannolikheter, hot och sårbarheter. Olika operatörer kan också ha olika strategier. För att åstadkomma en hög tillgänglighet kan de till exempel antingen välja att bygga en hög robusthet genom redundans och diversitet, eller att i stället satsa på resiliens och se till att nätet kan lagas snabbt vid ett avbrott. Specifika krav på redundans och diversitet kan vara motiverade om organisationen har behov av hög robusthet eller har behov av att stärka motståndskraften mot specifika hot.

Det är inte praktiskt eller ekonomiskt genomförbart att alltid köpa tjänster med hög redundans och diversitet i alla delar. Och även för en tjänst med mycket hög redundans och diversitet kvarstår ofta sårbarheter på systemnivå som i värsta fall kan orsaka avbrott, till exempel i operatörens interna it-system, nätfunktioner eller organisation. Det bör alltså inte ses som en universallösning utan som ett av flera verktyg för att åstadkomma säkerhet.

Sammanfattning:

- ✓ **Redundans och diversitet är viktigt för att inte enstaka fel ska leda till avbrott i tjänsten.**
- ✓ **Vilken redundans och diversitet som finns inbyggd i nät och tjänster varierar. Större stråk och centrala delar av nät är ofta byggda med redundans och geografisk diversitet.**
- ✓ **Redundans och diversitet i accessnät kan i vissa fall erbjudas på begäran av kunden. Att åstadkomma fysisk diversitet för en trådbunden access kräver inte sällan att nätet byggs om, vilket kan vara kostsamt.**

Exempel på redundans och diversitet för en trådbunden access



Säkerhet i användarens gränssnitt mot tjänsten

Att användarutrustningen, som utgör användarens gränssnitt mot operatörens nät, ger ett skydd mot intrång är viktigt för säkerheten.

En brandvägg används för att skydda användarens system och nät mot otillbörlig åtkomst. En sådan finns typiskt integrerad i den användarutrustning, till exempel en router eller en mobiltelefon, som utgör gränssnittet mot operatörens nät.

Brandväggens grundläggande funktion är att filtrera trafik och den brukar vara konfigurerad för att släppa igenom trafik som är initierad av användaren och hindra övrig trafik. Eftersom även viss trafik som inte initierats av användaren, till exempel ett inkommande telefonsamtal, behöver släppas igenom finns ofta kompletterande skydd som bygger på att trafiken analyseras på ett djupare plan än bara baserat på var den initierats. Till exempel genom att brandväggen också analyserar och filtrerar trafik baserat på hur trafik till och från en viss applikation borde bete sig.

För att reducera angreppsytan bör användarutrustning vara konfigurerad så att tjänster och protokoll som organisationen inte behöver är inaktiverade. Detta kallas härdning och går att läsa mer om i Nationellt cybersäkerhetscenters (NCSC) vägledning som vi nämner i lästipsen i slutet av vägledningen.

Det är viktigt att användarutrustning och brandvägg kontinuerligt hålls uppdaterade för att upprätthålla skyddet i takt med att nya sårbarheter och hot uppstår och upptäcks. Det är viktigt att tillverkaren av användarutrustningen kontinuerligt arbetar med säkerheten och tar fram uppdaterad mjukvara, och att denna sedan installeras på användarens utrustning. Vem som ansvarar för att förvalta användarutrustningen kan variera. I vissa fall är det operatören och i andra fall är det användaren själv eller en annan leverantör.

Sammanfattning:

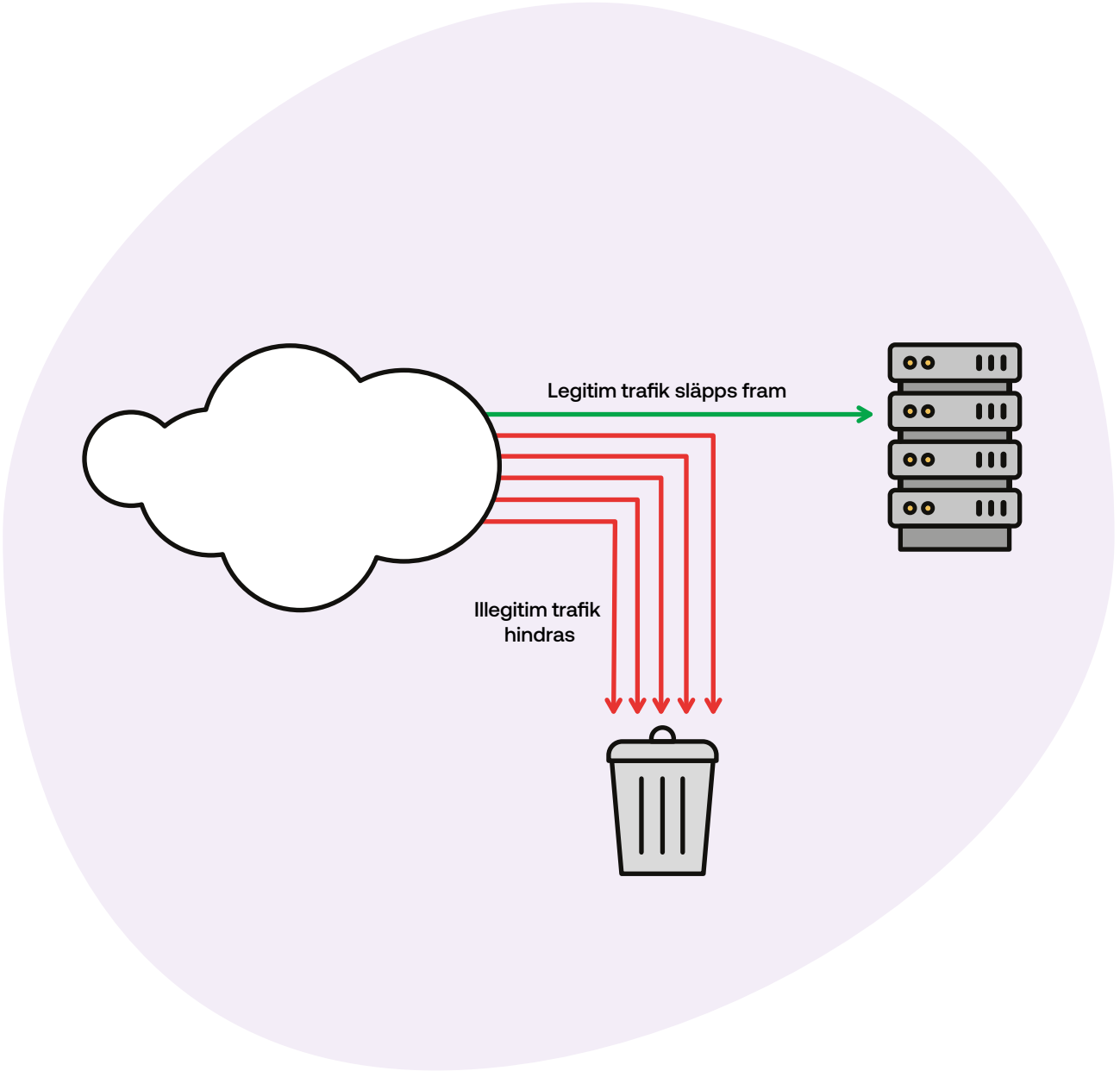
- ✓ **Säkerheten i den användarutrustning som utgör gränssnittet mot operatörens nät är viktig.**
- ✓ **Användarutrustning och brandvägg behöver förvaltas och hållas uppdaterade.**

Skydd mot överbelastnings-angrepp

Ett överbelastningsangrepp, DDoS (Distributed Denial of Service), innebär att en så stor mängd trafik skickas att det anslutna systemet överbelastas och inte kan uppfylla sin uppgift.

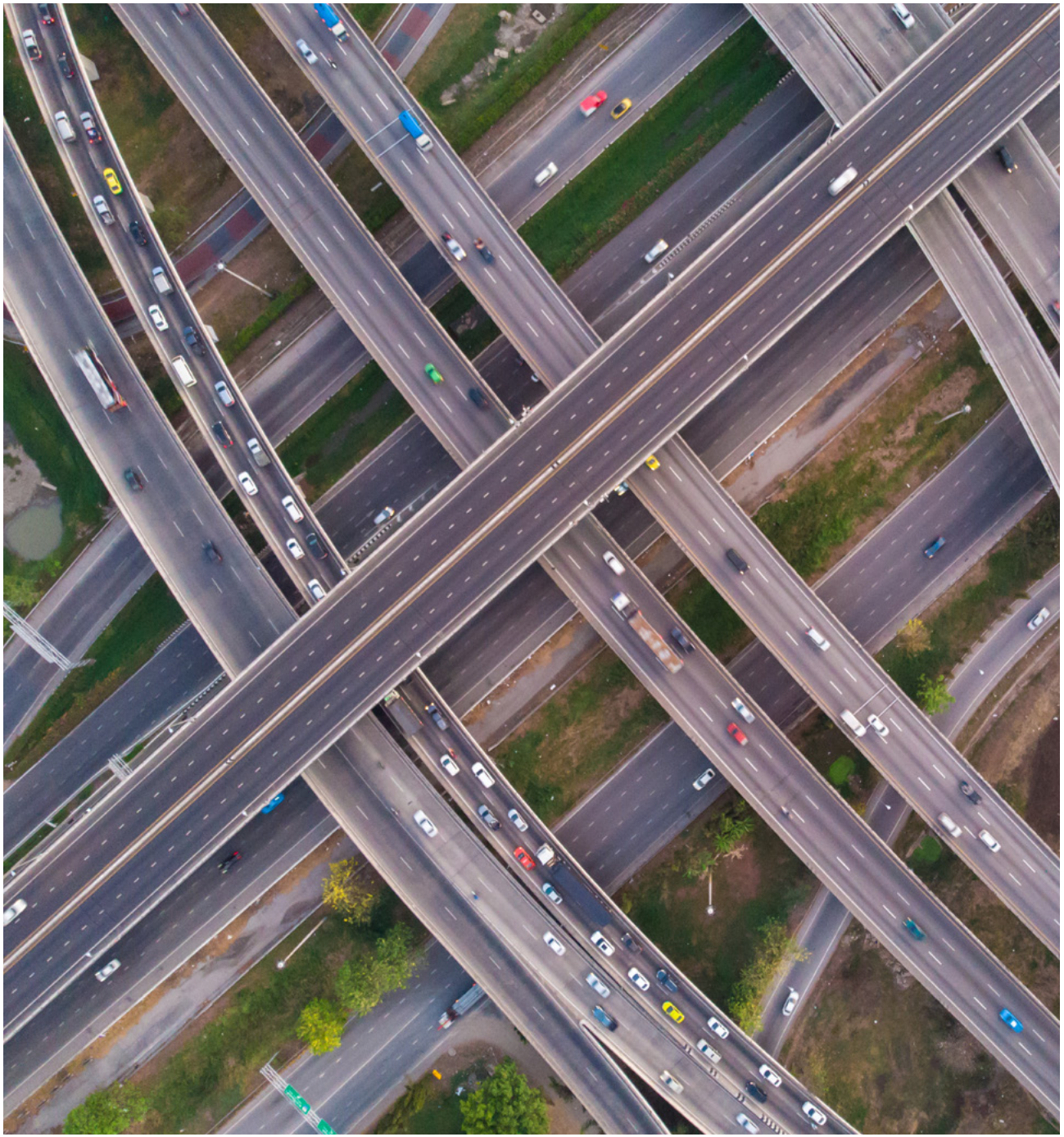
Överbelastningsangrepp kan hota tillgängligheten för system som är anslutna till internet. Angrepp kan till exempel riktas mot organisationens webbsajt eller internetanslutna applikationer. Tänk på att organisationen kan drabbas även om den inte är mål för angreppet, till exempel om någon annan aktör som använder samma server angrips.

Det finns metoder för att mildra konsekvenserna av sådana angrepp, till exempel att absorbera, filtrera och blockera trafik som bedöms vara illegitim. Eftersom ett angrepp kan omfatta mycket stora trafikvolymer behöver skyddet typiskt implementeras så att illegitim trafik hindras innan den når användaren. Tjänster för att skydda mot överbelastningsangrepp erbjuds såväl av operatörer som av vissa andra typer av leverantörer. CERT-SE (Sveriges Computer Emergency Response Team) har råd om hantering av överbelastningsattacker på sin webbsajt, se lästipsen i slutet av denna vägledning.



Sammanfattning:

- ✓ **Tillgängligheten i system som är anslutna till internet kan hotas av överbelastningsangrepp.**
- ✓ **Det finns metoder för att mildra konsekvenserna av sådana angrepp.**
- ✓ **CERT-SE (Sveriges Computer Emergency Response Team) har råd om hantering av överbelastningsattacker på sin webbsajt, se lästipsen i slutet av denna vägledning.**



Att separera trafik i privata nät

Med ett privat nät kan organisationens trafik avgränsas från andra användares trafik. Om organisationen behöver ett privat nät eller inte, och i så fall vilken typ av lösning, bör i första hand styras av behovet av tillgänglighet, konfidentialitet, riktighet och autenticitet.

Privata nät skapas oftast med logisk separation så att användaren får ett eget virtuellt privat nät, ett VPN.

Med ett VPN kan kryptering, signering och kontrollfunktioner användas för att skapa ett skydd för konfidentialitet, riktighet och autenticitet.

Ett VPN kan, som vi nämnt tidigare i vägledningen, vara nätbaserat eller ändpunktsbaserat. Med nätbaserade VPN kan i vissa fall extra funktioner för att skydda tillgängligheten läggas till. En operatör kan erbjuda en viss dedikerad överföringskapacitet och överföringskvalitet på ett sätt som inte är möjligt med en ett rent ändpunktsbaserat VPN.

Vissa typer av VPN gör det möjligt att analysera och styra användarens trafik i högre grad. Till exempel finns det lösningar där säkerhetsfunktioner kan implementeras baserat på vilken applikation trafiken hör till.

Ett ändpunktsbaserat VPN kan använda internet för sin transport. Det har då samma förutsättningar som annan transport över internet.

Sammanfattning:

- ✓ **Med privata nät, vanligtvis i form av VPN, kan organisationens trafik avgränsas från andra användares trafik.**
- ✓ **Olika typer av VPN kan ge olika sorters säkerhetsfunktioner. Om organisationen behöver ett privat nät eller inte, och i så fall vilken typ, bör i första hand utgå från behovet av tillgänglighet, konfidentialitet, riktighet och autenticitet.**

Onödiga beroenden och komplexitet

Elektronisk kommunikation är i sig ett komplext system där många olika delar ska passa samman. Tjänster som internetanslutning, VPN-tjänster och telefoni kan realiseras på olika sätt och hur det görs påverkar komplexiteten. Hur tjänsten realiseras påverkar också hur pass beroende den blir av funktioner som kan vara sårbara. För tillämpningar med behov av hög säkerhet bör strävan vara att försöka undvika sådan komplexitet och sådana beroenden som inte är nödvändiga. Det kan betyda att en avvägning behöver göras mellan funktion och säkerhet.

Till stor del kan detta åstadkommas med krav på tjänstens säkerhet och andra övergripande funktionella krav. Men det kan i vissa fall också vara relevant att ställa specifika krav för att reducera komplexitet och beroenden.

Några exempel på hur komplexitet och beroenden kan variera:

- Många led av underleverantörer innebär en ökad komplexitet och att tekniska och organisatoriska beroenden uppstår som kan påverka säkerheten.
- En telefonitjänst är beroende av applikationer och information hos operatören. Om en kontaktcenterlösning eller växelfunktionalitet dessutom läggs till innebär det sannolikt att komplexiteten ökar. Om telefonitjänsten inte fungerar självständigt utan växel- eller kontaktcenterfunktionen innebär det också ett ökat beroende.
- En trådbunden anslutning kan kopplas direkt från operatörens router till användaren eller passera via en eller flera switchar längs vägen. Det förstnämnda brukar kallas för dedikerad fiber och kan innebära ett lägre antal potentiella felkällor.

Sammanfattning:

- ✓ **För tillämpningar med behov av hög säkerhet bör ni försöka undvika komplexitet och beroenden som inte är nödvändiga.**
- ✓ **I vissa fall kan det betyda att en avvägning behöver göras mellan funktion och säkerhet.**

Redundans och diversitet med flera olika tjänster

Genom att ställa höga krav vid köp av en tjänst kan en hög säkerhet uppnås, men viss risk som är specifik för hur tjänsten produceras kommer alltid att finnas. Det kan i vissa fall vara lämpligt att stärka säkerheten i organisationens elektroniska kommunikationslösning som helhet genom att sprida tjänsteinköpen så att flera olika produktionssätt används.

Det kan göras för att skapa extra redundans i särskilt viktiga tillämpningar eller för att sprida risker genom att fördela organisationens tjänsteinköp. Diversifiering kan göras genom att köpa flera olika typer av tjänster från en operatör, eller att köpa från flera olika operatörer. Görs det på rätt sätt kan den sammantagna lösningen bättre motstå påfrestningar än en mer enhetlig lösning. Det förutsätter att den tillkommande logistiska och administrativa kostnaden inte överväger de potentiella fördelarna utifrån ett helhetsperspektiv och att den ökade komplexiteten inte i sig ger nya säkerhetsrisker.

Exempel på hur köp av tjänster med olika produktionssätt kan användas för redundans i särskilt viktiga tillämpningar:

- Att köpa två uppsättningar av tjänsten, varav en via en trådbunden access och en via mobilnätet.
- Att köpa två uppsättningar av tjänsten, från två olika operatörer

Exempel på hur köp av tjänster med olika produktionssätt kan användas för att minska risken att flera tillämpningar i verksamheten drabbas samtidigt vid en incident:

- Att köpa internetanslutning av en annan operatör än den som tillhandahåller telefonin.
- Att köpa internetanslutning med en trådbunden access och telefoni med en access via mobilnätet.
- Att fördela organisationens inköp av telefoni eller internetanslutning mellan flera olika operatörer.

För att detta ska ge effekt är det viktigt att inköpen av de olika tjänsterna verkligen ger en diversitet, alltså att de verkligen skiljer sig åt ur ett riskperspektiv. Det är inte möjligt för en användare att identifiera alla likheter och olikheter i produktionssätt.

Men utöver vilken operatör som tillhandahåller tjänsten kan ni sannolikt urskilja typ av access och typ av övergripande teknisk lösning.

En trådbunden signal är till exempel sårbar för grävskador på kabeln men inte för radiostörningar, medan det omvända gäller för en trådlös signal. Tjänster via mobilnät har flera skillnader jämfört med tjänster med trådbunden anslutning. Men tänk på att ett mobilnät ofta till stor del är trådbundet bortom accessnätet och ofta också har flera gemensamma sårbarheter med trådbundna nät.

Vid köp av tjänster från flera olika operatörer är det ur detta perspektiv viktigt att produktionssätten skiljer sig mellan operatörerna. Det kan finnas stora olikheter mellan olika operatörer i tekniska lösningar, fabrikat på utrustning, fysiskt nät, personal, processer, it-system, underleverantörer med mera. Men många operatörer har också gemensamma beroenden och sårbarheter.

Om tjänster ska köpas av två olika operatörer för att åstadkomma diversitet är det viktigt att ta reda på om de faktiskt skiljer sig åt i viktiga aspekter, till exempel:

- Är de två operatörerna verkligen olika organisationer med olika personal, it-system och processer eller är det två olika varumärken hos samma operatör?
- Finns det stora likheter mellan de två operatörernas nät, till exempel att de använder samma underleverantörs nät eller nyttjar varandras nät i stor utsträckning?

Observera att det är mycket svårt att säkerställa att vissa aspekter skiljer sig mellan två olika operatörer. Till exempel är det ofta svårt att utan tvivel säkerställa fysisk diversitet mellan två förbindelser hos olika operatörer.

Sammanfattning:

- ✓ **En tjänst har alltid vissa risker kopplat till hur den produceras. Det kan i vissa fall vara lämpligt att sprida inköpen så att flera olika produktionssätt används.**
- ✓ **Det kan göras för att skapa extra redundans i särskilt viktiga tillämpningar eller att för att sprida risker genom att fördela organisationens tjänsteinköp. Diversitet kan skapas genom att köpa flera olika typer av tjänster från en operatör, eller att köpa från flera olika operatörer**
- ✓ **Diversitet kan medföra ökad administration, kostnad och komplexitet och behöver därför vara väl genomtänkt.**
- ✓ **För att diversiteten ska ha någon effekt är det viktigt att de olika tjänsterna verkligen skiljer sig åt ur ett riskperspektiv.**

Begreppsförklaring

Här följer en kortfattad förklaring av vad som menas med de begrepp som används i denna vägledning. Observera att vissa av begreppen rättsligt och mer utförligt definieras i lag och att vissa begrepp kan ha en annan betydelse i andra sammanhang.

Access – anslutning till ett elektroniskt kommunikationsnät. Den del av nätet där detta sker kallas för accessnät.

Användarorganisation – Ett företag, en kommun, en myndighet eller annan organisation som använder en elektronisk kommunikationstjänst.

Användarutrustning – den utrustning som utgör användarens gränssnitt mot operatörens nät. Till exempel en dator, router eller mobiltelefon.

Applikation – En logisk funktion i mjukvara. Används bland annat i produktionen av elektroniska kommunikationstjänster.

Autenticitet – att uppgifter om informationens ursprung, till exempel vilket telefonnummer som ringer, inte förvanskas utan är korrekta.

Cybersäkerhet – All verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare och andra berörda personer mot en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka dessa. (rättslig definition finns i artikel 2.1 i EU förordning 2019/881)

Distribuerad – Utspridd på flera platser.

Diversitet – mångfald och inbyggda olikheter som gör att hela systemet inte är sårbart för samma sorts händelser.

Elektroniskt kommunikationsnät – ett system för överföring och dirigering av elektroniska signaler, oberoende av vilken typ av information som överförs. (rättslig definition finns i 1 kap §7 LEK)

Elektronisk kommunikationstjänst – en tjänst som tillhandahålls via elektroniska kommunikationsnät och som möjliggör informationsutbyte mellan personer, överföring av signaler eller anslutning till internet. (rättslig definition finns i 1 kap §7 LEK)

Hot – något som kan orsaka, eller bidra till att orsaka, en incident.

Incident – en oönskad händelse som ger en negativ inverkan på tillgängligheten, konfidentialiteten, riktigheten eller autenticiteten, eller på förmågan att motstå sådana händelser.

IP-adress – En adress som används för att kunna dirigera IP-paket enligt internetprotokollet.

IP-paket – Information som förpackats för överföring enligt internetprotokollet.

Konfidentialitet – att informationen som överförs och uppgifterna om själva kommunikationen, till exempel vilka parter som kommunicerar, skyddas mot obehörig åtkomst.

Kontinuitetsplanering – Planering för att upprätthålla prioriterad verksamhet trots störningar. Kallas även business continuity planning (BCP).

Kryptering - omvandling av information från begriplig klartext till en form som är obegriplig för obehöriga.

LEK – Lag (2022:482) om elektronisk kommunikation

Moln – En samling servrar, ofta distribuerade, som är tillgängliga via ett nätverk.

Molntjänst – En tjänst som ger tillgång till en skalbar och elastisk samling av gemensamma resurser i ett moln. (definieras rättsligt i artikel 6 i NIS2-direktivet)

MSB – Myndigheten för samhällsskydd och beredskap

NIS2-direktivet – EU-parlamentets och rådets direktiv 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148

Operatör – den som tillhandahåller ett elektroniskt kommunikationsnät som i huvudsak används till att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster. (rättslig definition finns i 1 kap §7 LEK)

Privat nät - ett nät som inte är tillgängligt för allmänheten. Med privata nät kan viss trafik, till exempel för olika användare, separeras fysiskt eller logiskt.

PTS Säkerhetsföreskrifter – Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2022:11) om säkerhet i nät och tjänster

Radiospektrum – ett utrymme för radiosignaler med vissa frekvenser.

Redundans – ett överskott av resurser, så att en funktion kan upprätthållas även om en enskild del slås ut.

Reservkraft – Utrustning som tillfälligt kan upprätthålla elförsörjning när det är avbrott i den ordinarie elnätsanslutningen. Det kan exempelvis vara batterier eller dieselgeneratorer.

Resiliens – förmåga till återhämtning och att klara av förändringar.

Riktighet – att informationen överförs utan att förvanskas.

Risk – en sammanvägning av sannolikheten att en oönskad händelse inträffar och konsekvenserna den i så fall får.

Robusthet – härdighet, en förmåga att stå emot påfrestningar.

Router – en typ av utrustning som används i elektroniska kommunikationsnät för att dirigera trafik i form av IP-paket.

Server – En fysisk eller virtuell dator som tillhandahåller applikationer eller lagring av information.

Säker elektronisk kommunikationstjänst – En elektronisk kommunikationstjänst som fungerar - med avseende på tillgänglighet, konfidentialitet, riktighet och autenticitet - trots oönskade händelser. (rättslig definition finns i 1 kap §7 LEK)

Tillgänglighet – att kommunikationstjänsten är tillgänglig för användning, med de egenskaper som överenskommits.

Transport – förflyttning av information genom ett elektroniskt kommunikationsnät. Den del av nätet där detta sker kallas för transportnät och binder samman stadsdelar, städer, regioner och länder.

Trådbunden elektronisk kommunikation – kommunikation via kablar som innehåller trådar av optisk fiber eller koppar, som bär lasersignaler eller elektriska signaler.

Trådlös elektronisk kommunikation – kommunikation som inte är bunden till en tråd och som vanligtvis sker via radiosignaler.

VPN – ett virtuellt privat nät. Baseras på virtuell (logisk) separation av trafik med hjälp av så kallade tunnlar. Med hjälp av kryptering kan konfidentialitet skyddas.

Lästips

Cybersäkerhet i Sverige – del 1 och 2 (NCSC)

Nationellt cybersäkerhetscenters rapport om cybersäkerhet i Sverige, del 1 (hot, metoder, brister och beroenden) och del 2 (rekommenderade säkerhetsåtgärder).

www.ncsc.se/publikationer/

Säkerhetsincidenter och integritetsincidenter på området elektroniska kommunikationer 2023, PTS-ER-2024-9 (PTS)

PTS har i denna rapport sammanställt och grupperat rapporterade incidenter under 2023 som är rapporteringspliktiga enligt Lag (2022:482) om elektronisk kommunikation.

https://pts.se/sakerhet-och-integritet/sakerhet-i-nat-och-tjanster/sakerhetsincidenter-ochintegritetsincidenter-pa-omradetelektroniska-kommunikationer2023-pts-er-20249/

Årsrapport IT-incidentrapportering 2023 (MSB)

Myndigheten för samhällsskydd och beredskaps årsrapport om IT-incidenter som rapporterats av statliga myndigheter och leverantörer av samhällsviktiga och digitala tjänster.

www.msb.se/sv/publikationer/eu-forandrar-cybersakerhetsomradet--arsrapport-it-incidentrapportering-2023/

Internetaccess, definition (Internetstiftelsen)

En rapport med syftet att skapa en gemensam uppfattning av vad internetaccess är, definiera viktiga begrepp och ge upphandlande organisationer en översikt om krav som kan ställas.

internetstiftelsen.se/app/uploads/2019/06/Internetstiftelsen_Internetaccess_Definition_Version_10_A4.pdf

Upphandla informationssäkert – en vägledning (MSB)

Myndigheten för samhällsskydd och beredskaps rapport från 2018 med vägledning om arbete med informationssäkerhet inför, under och efter en upphandling.

www.msb.se/sv/publikationer/upphandla-informationssakert--en-vagledning/

PTS.se

Post- och telestyrelsens webbsajt innehåller en mängd information inom området elektronisk kommunikation.

www.pts.se

Kontinuitetshantering (MSB)

Myndigheten för samhällsskydd och beredskaps samlade information om kontinuitetshantering.

msb.se/kontinuitetshantering

Informationssäkerhet, cybersäkerhet och säkra kommunikationer (MSB)

Myndigheten för samhällsskydd och beredskaps samlade information om Informationssäkerhet, cybersäkerhet och säkra kommunikationer.

www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/

Råd och stöd för att förebygga och hantera IT-säkerhetsincidenter (CERT-SE)

CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja det svenska samhället i arbetet med att hantera och förebygga it-säkerhetsincidenter. På webbsajten finns bland annat råd för förebyggande och hantering av överbelastningsangrepp.

cert.se/rad-och-stod/

Upphandlingsmyndigheten.se

Upphandlingsmyndighetens webbsajt innehåller bland annat en vägledning om inköpsprocessen och stöd vid upphandling av samhällsviktig verksamhet.

upphandlingsmyndigheten.se

Kammarkollegiets ramavtal inom IT och telekom (Kammarkollegiet)

Ramavtal för bland annat telefoni- och datakommunikationstjänster, vänder sig till statliga myndigheter.

www.avropa.se/ramavtal/ramavtalsomraden/it-och-telekom/

Lag (2022:482) om elektronisk kommunikation

www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482/

PTS föreskrifter och allmänna råd om säkerhet i nät och tjänster, PTSFS 2022:11

https://pts.se/regelbibliotek/foreskrifter-och-allmanna-rad-202211-om-sakerhet-i-nat-och-tjanster/

PTS-ER-2024:23

ISSN
1650-9862

Produktion
Make Your Mark / OTW
Foto: Adobe Stock

Post- och telestyrelsen
Box 6101
102 32 Stockholm

Telefon
08-678 55 00

Mail
pts@pts.se

Web
www.pts.se