Celab
COMMUNICATIONS

Guide till robusta kommunikationssystem

Hur stärker man kommunikationssystem för att stå emot utmaningarna under incidenter, kris och krig?

Guide till robusta kommunikationssystem

Hur stärker man kommunikationssystem för att stå emot utmaningarna under incidenter, kris och krig?

Svaret är - det är helt individuellt! Beroende på er verksamhet, er nuvarande kommunikationsmiljö och era krav så krävs helt olika förberedelser och åtgärder.

Med robust kommunikation avser vi system som kan upprätthålla tillräcklig/godtagbar funktion även vid störningar, avbrott eller belastning.

Denna artikel ämnar till att ge er en vägledning i olika tankesätt som kan hjälpa er att utveckla och/eller komplettera era kommunikationssystem för att förbättra motståndskraften mot potentiella hot – för att kunna leva upp till såväl interna som externa krav och förväntningar.

Den här artikeln är en del av en serie som skall hjälpa er "skottsäkra" er verksamhetskritiska kommunikationsmiljö. Vi rekommenderar att ni tar del av artiklarna i följande ordning.

1. Introduktion till beredskapskommunikation - Varför preparera?
2. Guide till riskanalyser för kommunikationssystem - Vad kan gå fel?
3. **Guide till robusta kommunikationssystem - Vad kan vi göra åt det? (denna artikel)**
4. Guide till pålitlig reservkommunikation - Vad gör vi när det ändå inte räcker till?

Syftet med artikelserien i stort är att ge er ett antal "linser" med vilka ni kan beskåda er kommunikationsmiljö för att kunna urskilja lämpliga åtgärder för just era förutsättningar.

Ni hittar alla våra artiklar på celab.se/kunskapsbank/artiklar.

Eftersom vägledningen endast berör hur man kan stärka upp befintliga system så förutsätts att ni har koll på de praktiska kommunikationsbehoven och funktionerna samt hur dessa tillhandahålls. Granskningen kan med fördel också involvera leverantör, konsult eller intern resurs med djupgående kompetens i de tekniska möjligheterna och begränsningarna.

Öka resiliensen

För att skapa motståndskraftiga system behöver systemet/systemen belysas ur flera olika perspektiv. Det gäller både övergripande och i detalj men också ur interna och externa synvinklar.

De olika perspektiven bör hjälpa er att;

- **Identifiera olika sätt att hantera och/eller eliminera utpekade risker från risk- och sårbarhetsanalyser.**
- **Hitta metoder för att förebygga onödiga framtida risker.**

1. Förstärkning

Första aktiviteten handlar om att urskilja systemets mer eller mindre uppenbara akilleshälar. Här behöver varje enskild komponent i systemet besiktigas och potentiellt bytas ut för att producera ett riktigt stabilt system.

Exempel på kontrollpunkter

Kategori	"Komponent"	Frågeställningar	Eventuella åtgärder
Mjukvaror	Firmware, Anti-virus, brandväggar...	Utgåva, version, specifikation?	Uppdatering, utbyte, uppgradering.
Aktiva delar	Basstationer, Repeatrar, Servrar, routers...	Ålder, specifikation, installation, skick?	Underhåll, reparation, utbyte, uppgradering.
Passiva delar	Antenner, kablar, kontakter...	Ålder, specifikation, installation, skick?	Reparera, byt ut, uppgradera.
Säkerhetsutrustning	Överspänningsskydd, jordfelsbrytare, åskledare...	Ålder, specifikation, installation, skick?	Reparera, byt ut, uppgradera.
Beroenden		Är systemet eller någon av dess delar beroende av andra system, tjänster eller leverantörer?	Se kommande avsnitt.

- **Med specifikation menas att verifiera att komponentens uttalade prestanda, kapacitet och kvalitet ligger i linje med kraven.**
- **Med skick menas komponentens allmänna hälsa avseende slitage, etc.**
- **Med installation menas att kontrollera att installationen är korrekt, välgjord och skyddad.**

2. Redundans

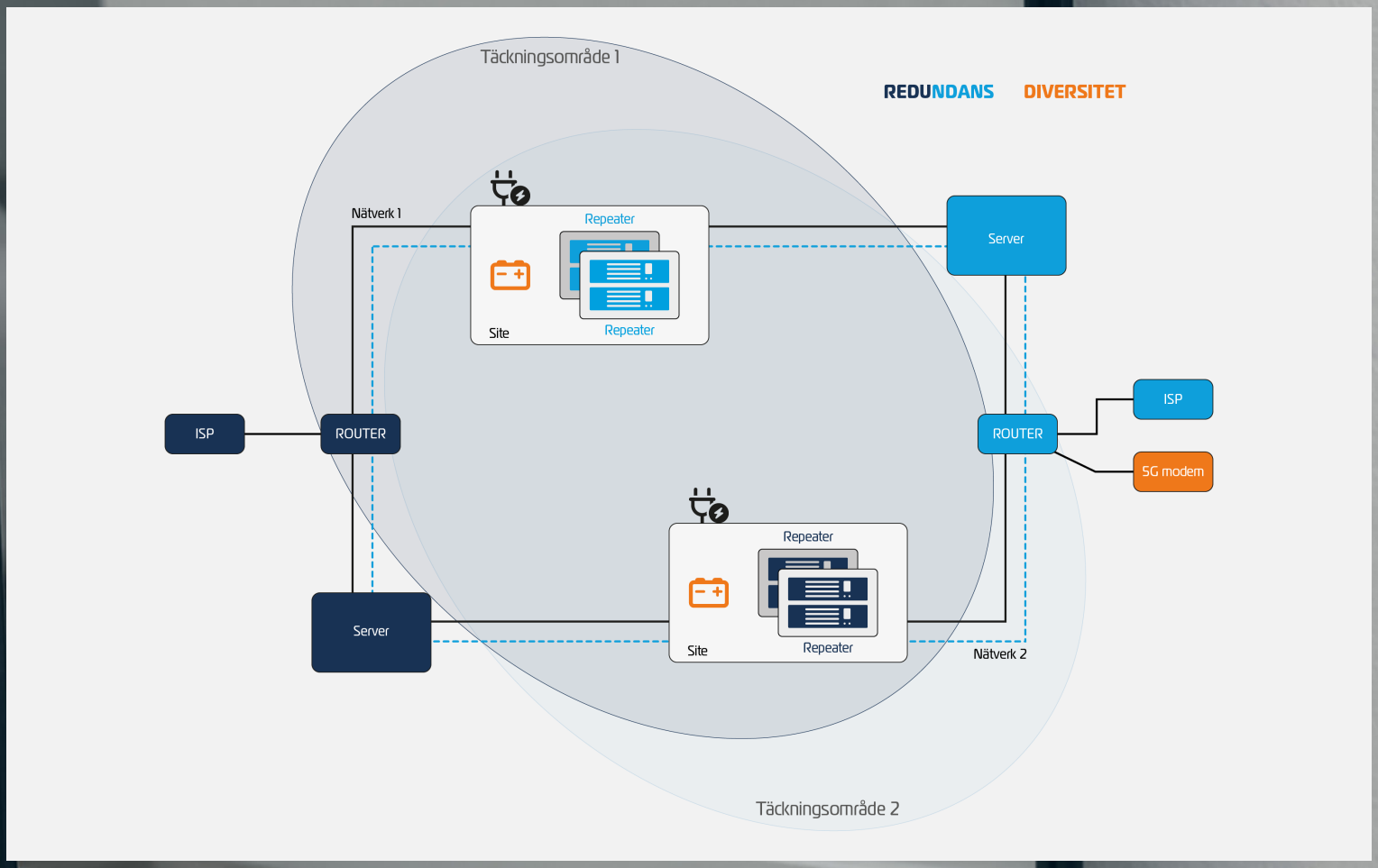
Redundans innebär att det finns extra resurser, reservvägar eller alternativa lösningar som kan ta över om något slutar fungera.

I ett kommunikationssystem kan redundans exempelvis bestå av dubbla nätförbindelser, reservkraft, flera servrar, alternativa basstationsplatser, extra terminaler eller ett separat reservkommunikationssystem.

Målet är inte alltid att funktionen ska vara helt oförändrad ur användarens perspektiv. I vissa fall räcker det att tillräcklig funktion bibehålls tills felet kan avhjälpas. Det viktiga är att ett enskilt fel inte omedelbart leder till att verksamheten tappar förmågan att kommunicera.

Exempel på kontrollpunkter

Kategori	Flaskhalsar	Eventuell dubblering
Beroenden	Internet-förbindelse	Parallell fiber-uppkoppling från annan ISP.
Aktiva delar	Basstationsplatser (Siter)	Dubbla siter - överlappande täckningsområden.
	Modem, server, router, etc	Speglad server-arkitektur. Virtuella miljöer.
Passiva delar	Nätverk, kablar, kontakter, etc	Parallella installationer. Överlappande täckningsområden.


Täckningsområde 1
REDUNDANS
DIVERSITET
Nätverk 1
Repeater
Server
Site
Repeater
ISP
ROUTER
ROUTER
ISP
5G modem
Repeater
Server
Site
Repeater
Nätverk 2
Täckningsområde 2

3. Diversitet

Diversitet innebär att redundanta lösningar skiljer sig åt i teknik, väg, leverantör, placering eller beroenden.

Syftet är att minska risken för gemensamma fel. Två förbindelser kan exempelvis vara redundanta, men om de går i samma kanalisation kan båda slås ut av samma grävarbete. Två abonnemang kan ge viss redundans, men om de använder samma underliggande mobilnät är diversiteten begränsad.

Diversitet handlar därför inte bara om att dubblera, utan om att säkerställa att reserven är tillräckligt oberoende från huvudlösningen.

Exempel på kontrollpunkter

Kategori	Flaskhalsar	Potentiell diversitet
Beroenden	Elförsörjning	UPS, batteribackup, back-up generator.
	Internet-förbindelser	Mobil- och/eller satellit-anslutning.
Aktiva delar	Basstationer	Systemspecifika funktioner
	Användarenheter	Direktläge (komradio)

4. Övervakning

Oavsett hur robust man än bygger ett system så finns det alltid en risk att enskilda beståndsdelar går ned eller krånglar. Därför är någon form av övervakning och larm avgörande för att undvika eller begränsa omfattningen och varaktigheten av eventuella bekymmer.

Automatisk övervakning kan finnas inbyggt i systemet eller behöva implementeras med hjälp av ytterligare hårdvara och/eller mjukvara. Oavsett så fungerar dessa (förenklat) på 2 huvudsakliga sätt.

- **Kontinuerlig: Systemet övervakas aktivt och varnar automatiskt vid fel.**
- **Health-check: Systemet tillfrågas regelbundet och svarar med ok eller fel.**

I de fall automatisk övervakning inte är möjligt eller tillräckligt så kan regelbundna manuella funktionskontroller enligt framtagen checklista behövas.

I kombination med tidigare nämnda åtgärder så möjliggör övervakning att reparationer, utbyten och andra avhjälpande åtgärder kan genomföras innan systemets funktion påverkas.

5. Separation

Geografisk separation

Detta är en förlängning av såväl diversitet och redundans som handlar om att speglade och/eller fail-over lösningar behöver vara separerade även fysiskt.

Det kan handla om att serverrum i olika byggnader, egna kabelvägar eller mix av trådade och trådlösa anslutningar - allt för att sprida sårbarheterna och därigenom risken.

Beroenden

Om man upptäckt ett eller flera beroenden som inte kan hanteras med hjälp av diversitets- eller redundanta åtgärder så kan dessa behöva vidare utredning.

Syftet är att utreda om beroenden bör och kan undvikas helt eller om tillfredställande robusthet kan uppnås "trots" det aktuella beroendet.

6. Åtkomlighet

Under denna rubrik skall åtkomsten till systemet - såväl fysiskt som virtuellt - bedömas och begränsas till vad som är absolut nödvändigt. Detta för att förhindra problem uppkomna av den mänskliga faktorn – såväl oavsiktligt eller med uppsåt.

"Ingång/Öppning"	Eventuell åtgärd
Virtuella portar	Stäng/Göm
Installationsutrymmen	Lås, begränsa tillträde.
Virtuella behörigheter	Begränsa behörigheter.

7. Servicenivå

Sista punkten är att se över eller teckna ett servicenivåavtal som försäkrar att underhåll, reparationer och andra felavhjälpande åtgärder kan genomförs i tillräcklig omfattning och tillräckligt skyndsamt. Oavsett om det gäller standard- eller skräddarsydda avtal så skall servicenivåerna spegla verksamhetens tolerans för avbrott och störning.

Ersättningsutrustning

Analysen kan sannolikt påvisa att enskilda komponenter behöver vara lättillgängliga för utbyte vid behov. Sådan ersättningsutrustning kan inkluderas i ett SLA men det kan också vara värt att undersöka om det är smidigare att ha dessa inköpta och förvarade lokalt.

Avslutning

Teknologival

Kan ert nuvarande system förbättras på alla nödvändiga punkter för att uppnå önskvärd eller godtagbar motståndskraft?

Om svaret är nej så kan det vara värt att utreda om det finns andra teknologier/system som låter er uppnå en godtagbar resiliens.

Reservkommunikation

Om ni gjort en komplett genomlysningen av er kommunikationsmiljö och genomfört alla möjliga åtgärder enligt denna artikel, men fortfarande inte kan släcka alla relevanta risker så kan ett Reservkommunikationssystem vara nödvändigt.

Mer om det i nästa artikel i serien - Guide till pålitlig reservkommunikation.

Om Celab

+46 (0)303 24 60 00
info@celab.se
https://celab.se

Celab Communications AB är ett företag inom Tången-gruppen som sedan starten 1978 upplevt stora framgångar inom verksamhetskritisk kommunikation.

Med det menar vi kommunikationslösningar för organisationer där sambandet är avgörande för verksamhetens framgång och/eller medarbetarnas säkerhet.

Företagets affärsidé är att tillhandahålla kommunikationssystem baserade på världsledande utrustning som genom vår unika kompetens utvecklas, förädlas och optimeras specifikt för våra kunder och deras unika verksamhet.

Celab COMMUNICATIONS

Huvudkontor Rollsbovägen 20, 442 40 Kungälv
Stockholm Elsa Brändströms gata 56, 129 52 Hägersten
Karlstad Lagergrens gata 2, 652 26 Karlstad