Celab
COMMUNICATIONS

Guide till riskanalyser för kommunikationssystem

Hur garanterar man att man inte missar något när man utvärderar sin kritiska kommunikationsmiljö?

Guide till riskanalyser för kommunikationssystem

Hur garanterar man att man inte missar något när man utvärderar sin kritiska kommunikationsmiljö?

Det korta svaret är dessvärre ”det går inte”, men genom att göra en grundlig och genomtänkt nulägesanalys kan vi minimera falsk trygghet och maximera motståndskraften i kommunikationen för att förbereda organisationen på bästa möjliga sätt.

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.

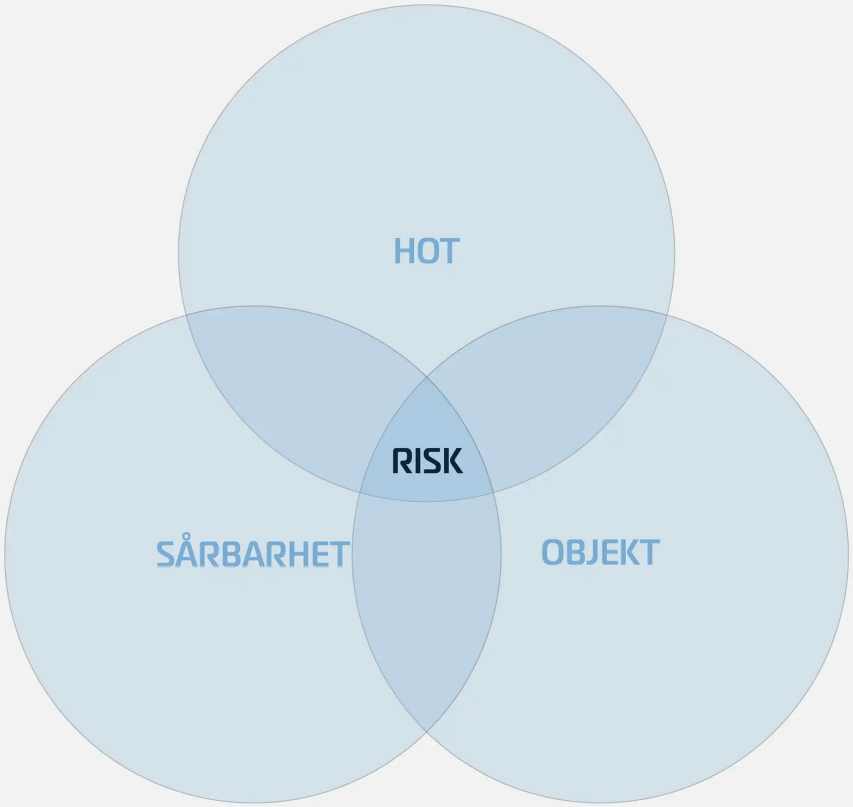
1. Introduktion till beredskapskommunikation - Varför preparera?
2. **Guide till riskanalyser för kommunikationssystem - Vad kan gå fel? (denna artikel)**
3. Guide till robusta kommunikationssystem - Vad kan vi göra åt det?
4. Guide till pålitlig reservkommunikation - Vad gör vi när det ändå inte räcker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

Risk- och sårbarhetsanalys

Precis som för alla riskanalyser syftar denna del i processen till att inventera och bedöma risker och hot, men med specifikt fokus på er kommunikationsmiljö. Vi kan inte ge er svaren men med denna ”checklista” hoppas vi kunna hjälpa er att själva utforma en riskanalys och metodik som passar er verksamhet och er kommunikationsmiljö.



Hot	Potentiell incident utanför objektet som kan medföra påverkan.
Sårbarhet	Brist i det analyserade objektet som möjliggör ett hot.
Konsekvens	Påföljden om hotet realiseras.
Objekt	Systemet som granskas.
Risk	Variabel som utgör resultatet av bedömningen.

HOT → utnyttjar en → SÅRBARHET → som leder till → KONSEKVENS → vilket utgör en → RISK

Definiera objektet

Inledningsvis måste ni avgränsa er analys genom att bestämma vilket/vilka system som skall granskas genom att precisera systemet, dess beståndsdelar och avgränsningar – exempelvis ”TETRA-systemet” eller ”Privata mobilnätet”.

Det blir väldigt mycket enklare att fokusera på hot som är relevanta för det aktuella objektet om alla objekt och dess beståndsdelar är tydligt dokumenterade.

Identifiera hot

Ni behöver urskilja och lista samtliga potentiella händelser som kan begränsa eller eliminera er möjlighet att använda det aktuella objektet – stort som smått.

Detta innefattar alla potentiella faror - oavsett om de uppkommit på grund av olycka, oaktsamhet eller illvilja. Det spelar heller ingen roll om de beror på inre eller yttre omständigheter – ”allt” kan vara relevant och bör utvärderas och dokumenteras.

Tillvägagångssätt

Kartlägg objektet

Beskriv objektet, dess process, funktion och ingående delar.

Brainstorma hot

Sätt samman en grupp med olika kompentenser för att identifiera vad som kan gå fel?

Tillgängliga data

Finns det relevant statistik, dokumentation?

Ta hjälp

Kan ni få hjälp av interna experter, branschorganisationer, myndigheter, konsulter eller leverantörer?

Matris för hotbild

Kategori / Anledning	Exempel	Olycka	Oaktsamhet	Uppsåt
Tillgänglighet (Avbrott)	Strömavbrott, Inget internet, Låst system	Storm, Åsknedslag, Bugg	Kabelbrott, Urkopplad server, Felaktig hantering	Sabotage, Ransomware
Prestanda (Störning)	Dålig mottagning, Upptaget, Buffrande	Interferens från andra system, Hårdvarubrister	Underdimensionerad kapacitet och/eller komponent	Jamming, Överbelastnings-attack
Sekretess/ Integritet (Läckage)	Röjd information, Manipulerade data	Systemfel, Bugg	Bristande rutiner, Bristande behörighets-hantering	Spioneri, MiTM, Intrång, Phishing, Insider

I matrisen är potentiella hot grovt grupperade enligt den typ av problem som kan uppstå (Y-axeln) samt bakomliggande orsak (X-axeln).

Beroende på era förutsättningar så är de olika hoten mer eller mindre aktuella.

Utvärdera sårbarheter

Detta steg handlar om att evaluera objektets nuvarande svagheter – specifikt i relation till redan utpekade hot.

För varje enskilt hot behöver en eller flera Sårbarheter kopplas – alltså brister som de utvalda hoten kan exploatera för att realiseras.

Tillvägagångssätt

Kartlägg objektet

Granska specifikationer, ritningar, systembeskrivningar, etc

Tillgängliga data

Finns det information, mallar, best-practices m.m. att tillgå?

Ta hjälp

Kan ni få hjälp av säkerhetsexperter, myndigheter, leverantörer?

Bedömningsmatris för sårbarheter

Område / Signifikans >	Försumbar	Betydande	Akut
Tekniska	Acceptabel nödkraft	Otillräcklig nödkraft, Föråldrad firmware, Utgången antivirus, Otillräcklig kryptering	Single-point(s)-of-failures, Zero-day
Fysiska	Acceptabelt skalskydd	Otillräckligt skalskydd	Obefintligt skalskydd
Organisatoriska	Acceptabel lösenordshantering	Bristande behörighetshantering	Ingen behörighetshantering
Mänskliga		Social engineering	Enkla lösenord

Matrisen kan utökas med fler "nivåer" för att göra den mer finfördelad.

Bedöm konsekvenser

Nu är det dags att avgöra påföljden om era utpekade hot faktiskt besannas.

Även här måste påföljden utredas, värderas och dokumenteras för varje enskild risk. Eftersom konsekvensernas allvar kan skilja sig markant beroende på hur länge de pågår är det viktigt att väga in ett tidsperspektiv.

För strömavbrott kan det till och med vara fördelaktigt att behandla det som olika hot beroende på längd.

Ett annat tidsrelaterat perspektiv att fundera på är hur länge ni måste klara er själv innan yttre hjälp kan förväntas.

Bedömningsmatris för konsekvenser

Vad/Allvarlig-hetsgrad	Obefintlig	Begränsad	Måttlig	Allvarlig	Kritisk
Tillgänglighet (Avbrott)	-	Momentant strömavbrott	Kortvarigt strömavbrott	Långvarigt strömavbrott	"Permanent strömavbrott"
Prestanda (Störning)	-	Intermittenta störningar	Otillräcklig mottagning eller bandbredd	Bristande mottagning eller bandbredd	Ingen mottagning/ täckning eller bandbredd
Integritet / Sekretess (Läckage)	-	-	Förlust av känslig info	Förlust av konfidentiell info	Förlust av hemlig info

Matrisen kan utökas med fler "nivåer" för att göra den mer finfördelad.

"Den som bedriver samhällsviktig verksamhet ska – enskilt och i samverkan – stärka förmågan att med främst egna resurser upprätthålla de viktigaste samhällsfunktionerna i minst två veckor." - Ur Beredskap för företag - Om krisen eller kriget kommer.

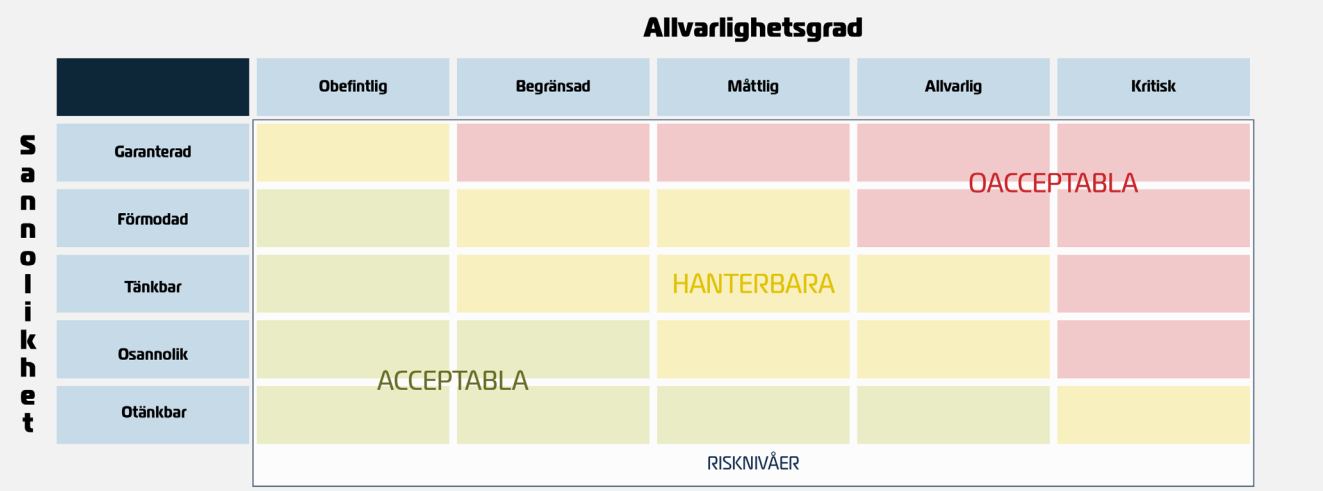
Värdera och prioritera risker

När ni vet vilka hot ni står inför, vilka sårbarheter ni besitter och vilka potentiella konsekvenser ni riskerar så kan ni slutligen fastställa Risknivåerna och således få en prioriteringslista att arbeta med.

Detta kan göras genom att vikta sannolikheten för att varje enskild Hot inträffar, viktat mot "allvarlighetsgraden" som just det hotet utgör.

Sannolikheten kan uppskattas genom att jämföra Hotet och Sårbarheten medan Allvarlighetsgraden är kopplat till Konsekvensen.

Bedömningsmatris för Risknivåer



Matrisen kan anpassas med fler eller färre grader och sannolikheter.

Om man sätter ett värde för de olika steg på respektive axel kan siffrorna multipliceras för att få ett enkelt sätt att prioritera sina insatser.

Avslutning

Döda vinklar

Det är "lätt" att förbereda sig för scenarion som ni själva eller någon annan i organisationen upplevt men, det är minst lika viktigt att preparera för dem ni aldrig ställts inför.

Det finns 3 typer av riskmedvetenhet.

- **De risker ni känner till och har kontroll över.**
- **De risker ni känner till men saknar kontroll över.**
- **De risker ni varken känner till eller har kontroll över.**

För att täcka in samtliga kategorier behöver vi sannolikt tänka utanför boxen och föra en dialog med externa parter.

Nästa steg

När ni väl har sammanställt all data så har ni sannolikt en riktigt bra bild över er situation, era behov och nödvändiga åtgärder.

Om er analys påvisar;

Samtliga risknivåer är på en acceptabel nivå?

Grattis - Ingen vidare åtgärd är nödvändig.

Risker behöver hanteras eller elimineras?

Förbättra befintligt (ordinarie) kommunikationssystem

- **Se vår Guide till robusta kommunikationssystem.**

Trots insatser återstår oacceptabla risknivåer?

Anskaffa eller förbättra ett reservkommunikationssystem!

- **Se vår Guide till pålitlig reservkommunikation.**

Vissa risknivåer kan inte begränsas!

Anskaffa nytt ordinarie och/eller reservkommunikationssystem.

- **Kontakta oss för en översyn & behovsanalys.**

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