Malin Ekblad
Säkerhetschef
malin.ekblad@trelleborg.se

Kommunstyrelsen

Bilaga 4 b - NIS direktivet: riskanalys för informationssäkerhet

Leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ISO 27000-standarden. Även leverantörer av digitala tjänster ska vidta säkerhetsåtgärder för att hantera risker och säkerställa kontinuiteten.

NIS-regleringen gäller specifikt de nätverks- och informationssystem som den samhällsviktiga eller digitala tjänsten är beroende av, men grunderna i det systematiska och riskbaserade informationssäkerhetsarbetet är detsamma oavsett vilken eller vilka verksamheter som omfattas.

Att arbeta systematiskt innebär att regelbundet analysera verksamhetens krav, att införa ändamålsenliga säkerhetsåtgärder utifrån dessa krav, samt att kontinuerligt följa upp och förbättra skyddet. Med riskbaserat menas att säkerhetsåtgärderna ska vara anpassade till verksamhetens identifierade risker och behov, vilket ger ett ändamålsenligt skydd.

Informationssäkerhet för samhällsviktiga och digitala tjänster är tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. De är indelade i sju sektorer:

- energi
- transport
- bankverksamhet
- finansmarknadsinfrastruktur
- hälso- och sjukvård
- leverans och distribution av dricksvatten
- digital infrastruktur

Leverantör: en aktör som identifierats som en leverantör av samhällsviktiga tjänster.

Förslagsvis: leverans och distribution av dricksvatten eller energi.

Underleverantör: en aktör som förser en leverantör med varor eller tjänster och som inte står under direkt organisatorisk kontroll under leverantören.

Leverantören ska föra aktuella förteckningar över

- tillgångar i form av nätverksansluten hård- och mjukvara,
- förbindelser i form av kommunikationslänkar,

- beroenden till underleverantörer, och
- vilka delar av den egna organisationen (organisatorisk enhet)

som kan påverka säkerheten i den samhällsviktiga tjänsten. Förteckningarna ska omfatta en aktuell kartläggning av logiska samband och kommunikationer till och från systemkomponenter.

Genomgång av riskanalysens olika delar

Informationsklassning

I riskanalysen specificeras vilken information som finns i systemet. Informationen klassificeras enligt informationssäkerhetsprinciperna *konfidentialitet, riktighet, tillgänglighet och spårbarhet* (se klassificeringsmodell ovan). Utifrån klassificeringen får systemet ett skyddsvärde på respektive informationssäkerhetsprincip. Utifrån skyddsvärdet på systemet så rekommenderas lämpliga säkerhetsåtgärder.

Skyddsåtgärder

I skyddsåtgärderna bedöms bland annat åtkomst (behörigheter, autentisering eller stark autentisering), loggning, säkerhetskopiering, Anskaffning och utveckling av system, tredjepart/leverantörer, användarens ansvar, kryptering, rutiner för avvikelsehantering, drift, personuppgifter & kommunikation och nätverk.

Leverantören ska se till att nätverks- och informationssystem som används för leverans och distribution är logiskt eller fysiskt separerade från informationssystem eller nätverk som inte omfattas av motsvarande krav på informationssäkerhet.

Åtkomst till nätverks- och informationssystem som har betydelse för den samhällsviktiga tjänsten ska endast medges till den eller det som behöver sådan åtkomst för att kunna utföra sina arbetsuppgifter. Tilldelad behörighet ska begränsas till det som är nödvändigt. Leverantören ska ha fastställda regler för tilldelning, ändring och uppföljning av åtkomst och behörighet.

Leverantören ska se till att autentisering vid fjärråtkomst till informationssystem som har betydelse för den samhällsviktiga tjänsten baseras på flera faktorer (flerfaktorsautentisering).

Riskhantering

Vidare identifieras vilka risker som finns i systemet och risken klassificeras utifrån sannolikhet att något inträffar och konsekvens för verksamheten om risken inträffar. Sannolikheten att något kan inträffa är enligt följande:

1. Mycket Sällan – en gång på 10 år
2. Sällan - En gång på 1 år
3. Regelbundet – en gång på 1 månad
4. Ofta – en gång på 1 vecka

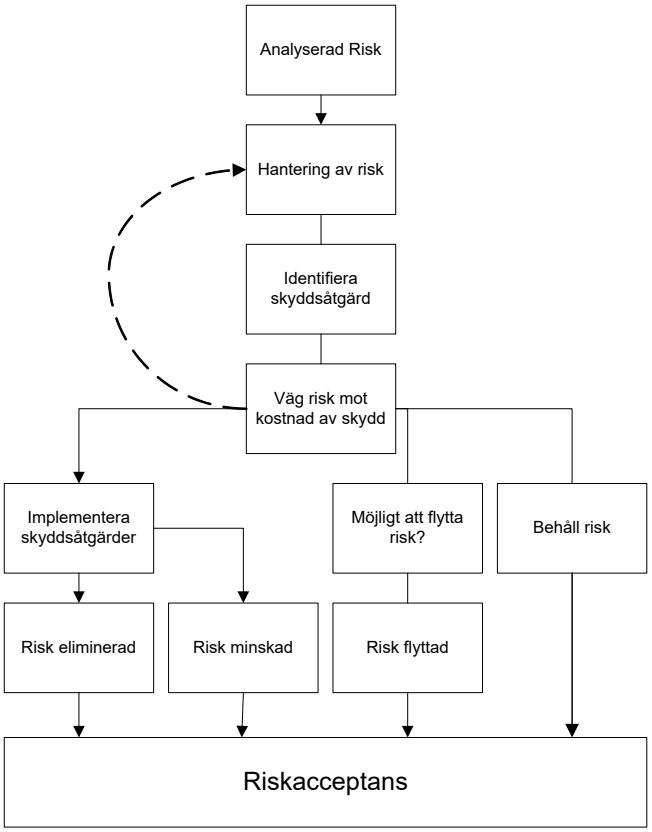
Konsekvensen är ett mått på den skada en risk skulle ha på verksamheten om den inträffar. Påverkan kan vara direkt eller indirekt, ekonomisk eller mänsklig. I modellen använder vi oss av nivåerna:

1. Försumbar – Kan innebära kostnader upp till max 10 000 kr
2. Måttlig – Kan innebära kostnader upp till max 100 000 kr
3. Betydande - Kan innebära kostnader upp till max 1 000 000 kr
4. Allvarlig - Kan innebära kostnader upp till max 30 000 000 kr

Utifrån denna klassificering får respektive risk ett riskvärde, där ett högre riskvärde innebär en högre risk.

	Mycket sällan	Sällan	Regelbundet	Ofta
Försumbar	1	2	3	4
Måttlig	2	4	6	8
Betydande	3	6	9	12
Allvarlig	4	8	12	16

Nästa steg i riskhanteringsprocessen är att hantera risker som identifierats och bedömts. En risk kan minskas, elimineras, flyttas eller accepteras. Målet är att inga risker skall accepteras utan att ett medvetet val gjorts kring detta. Bilden nedan illustrerar processen för riskhantering:



HUKI-analys

Därefter görs en HUKI-analys, som innebär att det utses en huvudansvarig för respektive risk, det utses vem som ska arbeta med risken (utförare), vem som behöver konsulteras för att arbeta med risken och vem man ska informera om vidtagna åtgärder.

Hur klarar systemet GDPR (Dataskyddsförordningen)

Därefter kontrolleras vilka personuppgifter som hanteras i systemet, att de stämmer överens med de behandlingar som är registrerade i kommunens registerförteckning, att biträdesavtal och sekretessavtal är skrivna samt huruvida systemet uppfyller lagkraven enligt dataskyddsförordningen (GDPR). Avslutningsvis analyseras behovet av backup för systemet (säkerhetskopiering), vilket ligger till grund för det avtal systemägaren ska ha med IT-avdelningen och/eller systemleverantören.

Rekommendation & summering

IT och informationssäkerhetssamordnaren ska vid riskanalysen lämna en rekommendation om huruvida de anser att systemet uppfyller kraven och om det bör driftsättas/får fortsatt användas inom kommunen.

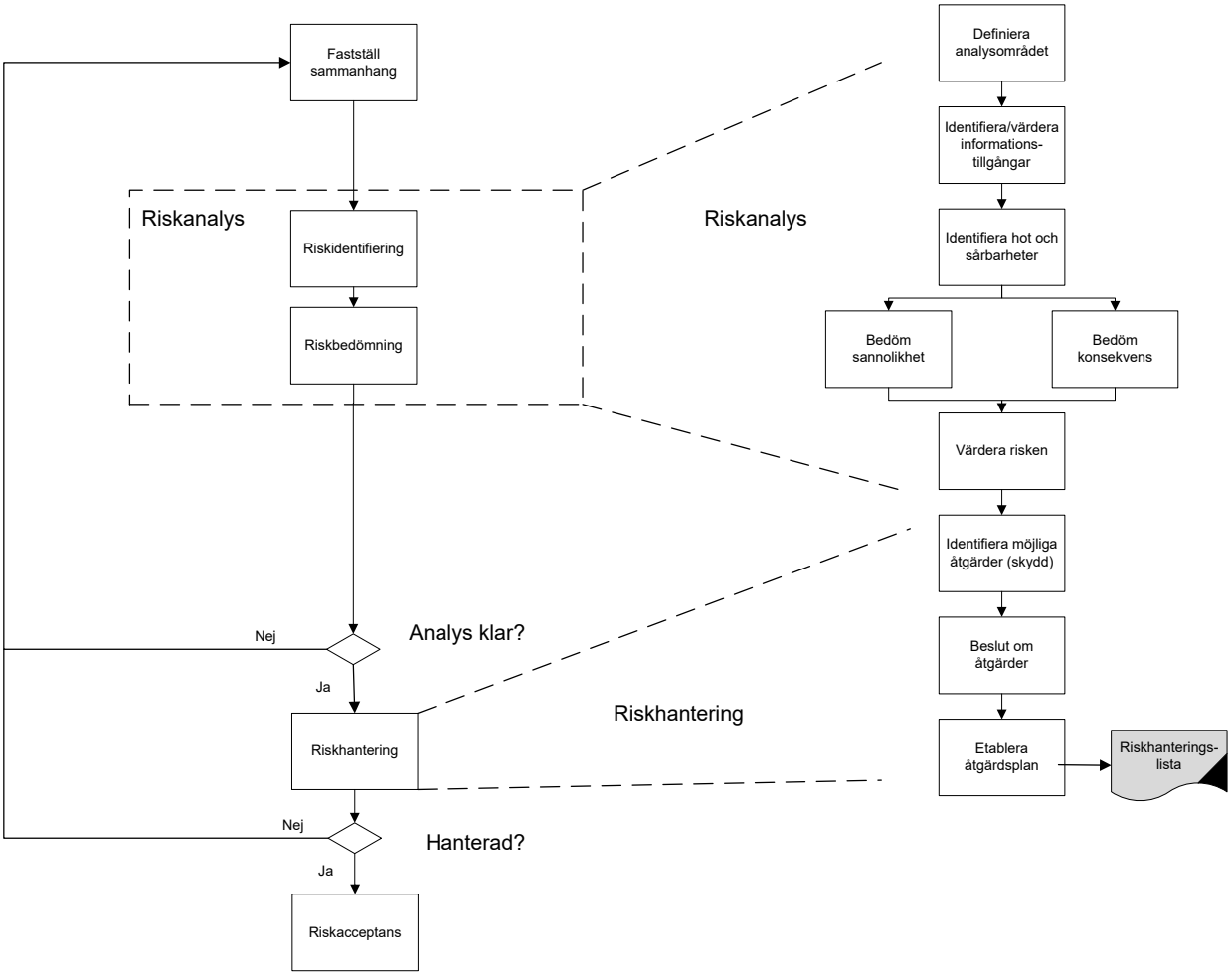
Vid negativ rekommendation ska detta informeras till ansvarig nämnd eller bolag som tar beslut om systemet ska få driftas eller inte.

Riskanalysen ska genomföras innan ett system köps in/börjar användas i kommunen. Analys ska fortlöpande göras en gång per år för samtliga system som hanterar personuppgifter eller verksamhetsinformation.

Det är systemägarens ansvar att riskanalysen genomförs och att rekommenderade åtgärder vidtas. Inledande riskanalys ska göras av systemägaren eller systemansvarig tillsammans med informationssäkerhetssamordnaren och utsedd medarbetare från IT-avdelningen.

Den årliga uppföljande riskanalysen ska vid behov göras av systemägaren eller systemansvarig tillsammans med informationssäkerhetssamordnaren och utsedd medarbetare från IT-avdelningen. Förekommer det inget behov av gemensam uppföljning kan systemägaren alternativt systemansvarig göra riskanalysen själv och informera informationssäkerhetssamordnaren samt IT-avdelningen om resultatet. Upphandling av nytt system ska ske i samråd med IT-avdelningen. Vid förändring i system, som exempelvis när ny information läggs till, ska detta rapporteras till IT-avdelningen.

Processkarta se nedan



Fem viktiga råd

1. Leverantör och underleverantörs kunskap om aktuell hotbild och säkerhetsfrågor.
2. Isolera och segmentera nätverk för SCADA- och automationssystem.
3. Inför säkrare rutiner för behörighetskontroll på individnivå. Kräv alltid tvåstegsautentisering för all inloggning på distans. Begränsa behörigheterna - tillåt inte mer än absolut nödvändigt.
4. Övervaka nätverken och säkerställ spårbarhet av allt som sker i nätverken.
5. Genomför kompletta backuper av alla kritiska system. Förvara backuper ”offline” så att de inte kan angripas och krypteras av ransomware (utpressningsprogramvara). Viktigt att även löpande testa att återställa data från backuper.