



Svar på interpellation från Marie Ericsson Drotte (LOK) om status för kommunens arbete med anpassning till NIS2

Fråga 1:

Hur ser det aktuella läget ut i Strängnäs kommuns arbete med att anpassa sig till den kommande cybersäkerhetslagen (NIS2)?

Svar:

Arbete pågår. Se punkt 4.

Fråga 2:

Vilka konkreta åtgärder har vidtagits sedan fullmäktiges beslut den 15 april 2024 för att omsätta riktlinjerna i praktiken?

Svar:

Vi har fokuserat på de delar som lagstiftaren varit tydligast med, vilket innebär ett intensifierat arbete med att bygga upp ett systematiskt och riskbaserat informationssäkerhetsarbete i hela kommunen, med särskilt fokus på våra samhällsviktiga tjänster.

Konkreta åtgärder:

- **Organisation och Styrning:** En organisation för informationssäkerhet har delvis inrättats med två personer som arbetar aktivt med dessa frågor. Enligt riktlinjen för informationssäkerhet skulle ett informationssäkerhetsråd inrättas, men det har ej skett eftersom FLG inte ansåg detta som nödvändigt. Arbetet med att upprätta en organisation pågår.
- **Riktlinje för informationssäkerhet** implementerades under våren 2024. Tillhörande styrdokument (tillämpningsanvisningar kommer att släppas inom kort och anpassas för ny lagstiftning). Dessa är under framtagande för att möta de högre kraven i kommande lagstiftningar.
- **Kompetensutveckling:** Obligatorisk utbildning i informationssäkerhet och dataskydd genomförts för all personal. En särskild utbildning i säkerhetsåtgärder är under framtagande för chefer och ledning (krav i nya lagen). MSB har nyligen annonserat underlag för kommande krav och innehåll.
- **Inventering och Klassning:** Ett omfattande arbete har genomförts med att inventera kommunens samtliga IT-system och informationstillgångar samt klassificera informationen utifrån krav på konfidentialitet, riktighet och tillgänglighet (KRT).



- **Risikanalyt:** Systematiska riskanalyser har genomförts för de mest kritiska verksamheterna/systemen för att identifiera och åtgärda sårbarheter.

Fråga 3:

Hur säkerställs att alla nämnder och förvaltningar tar fram och följer lokala handlingsplaner för informationssäkerhet, i enlighet med beslutet?

Svar:

Ansvar för informationssäkerheten ligger i enlighet med riktlinjerna på respektive nämnd. Kansliet har en samordnande, stödjande och uppföljande roll för att säkerställa en enhetlig och hög nivå i hela organisationen. Handlingsplanerna tas fram i samband med klassning i SKR:s Klassa och sammanställs för varje år och nämnd.

Exempel på säkerställande:

- **Mallar och Stöd:** Mallar för lokala handlingsplaner och metodstöd kommer att tas fram och distribuerats till alla kontor.
- **Utseende av roller:** Vissa kontor har utsett en kontaktperson som kommer att ingå i ett kommunövergripande nätverk. (Idag finns GDPR-samordnare som vi vill ska ingå i detta nätverk).
- **Uppföljning och rapportering:** Införande av en årlig rapporterings- och uppföljningsprocess (Ledningens genomgång¹) där varje nämnd redovisar status för sitt informationssäkerhetsarbete och efterlevnad av handlingsplanen till Kommunstyrelsen. Dessa underlag ska även rapporteras i det som kallas Ledningens genomgång (ISO-standard), MSB:s metodstöd och SKR:s metodstöd.
- **Revision:** Internrevisionen kommer att få i uppdrag att inkludera granskning av informationssäkerhetsarbetet och efterlevnaden av lokala handlingsplaner i sin revisionsplan.

Fråga 4:

På vilket sätt förbereder kommunen sig för att kunna uppfylla de nya lagkraven senast vid ikraftträdandet den 15 januari 2026?

¹ Ledningens genomgång är ett forum där Informationssäkerhetssamordnaren (CISO) tillsammans med utsedda specialister, enligt ISO-standard 27000 och MSB:s metodstöd, årligen rapporterar arbetet med informationssäkerhet för styrelsen (i detta fall kommunstyrelsen). Ledningens genomgång har enligt ISO-standard en färdig agenda.



Svar:

Kommunen har inlett ett proaktivt och strukturerat arbete för att implementera NIS2-direktivet (som blir den nya Cybersäkerhetslagen). Vi ser detta som en möjlighet att höja hela vår motståndskraft, inte bara ett regelefterlevnadsprojekt.

Förberedelser (NIS2):

- **Gap-analys (Nulägesanalys):** Vi har genomfört en analys för att identifiera skillnaden (gapet) mellan kommunens nuvarande informationssäkerhetsnivå och de krav som den nya Cybersäkerhetslagen (NIS2) ställer, särskilt gällande tekniska och organisatoriska säkerhetsåtgärder. Dessutom har en granskning skett på initiativ av kommunens samtliga nämnder där vi under november månad kommer att få ta del av resultatet av granskningen.
- **Säkerhetsåtgärder:** Fokus ligger på att implementera de obligatoriska säkerhetsåtgärderna, såsom robust incidenthantering (inkl. rapporteringsrutiner), leverantörskedjesäkerhet, åtkomstkontroll, kryptering och MFA (Multi-Factor Authentication).
- **Samverkan:** Aktivt deltagande i nätverk och stödstrukturer, som till exempel de som erbjuds av SKR (Sveriges Kommuner och Regioner) och MSB (Myndigheten för samhällsskydd och beredskap), för att dra nytta av nationella erfarenheter och metodstöd.

Fråga 5:

Vilka lärdomar drar kommunen av cyberangreppet mot Miljödata när det gäller beroendet av externa leverantörer?

Svar:

Angreppet mot Miljödata var en smärtsam påminnelse om att hela vår digitala leveranskedja är en del av vår egen säkerhet. Den viktigaste lärdomen är att vi måste ha en mycket strängare och mer proaktiv kontroll över våra externa leverantörer, särskilt de som hanterar kritisk information och system.

Exempel på lärdomar:

- **Riskbaserad Leverantörsgranskning:** Vi kommer förstärka rutinerna för riskanalys av leverantörer och deras underleverantörer, med fokus på deras förmåga att skydda vår information och upprätthålla tjänsternas tillgänglighet (krav på systematiskt arbete med säkerhet i leveranskedjan).



- **Tydligare Avtal:** Nya och omförhandlade avtal ska innehålla tydliga och mätbara säkerhetskrav, inklusive krav på incidentrapportering och rätten till revision av leverantörens säkerhetsarbete.
- **Beredskapsplaner:** Stärkt fokus på att utveckla och testa kontinuitetsplaner och återställningsförmåga för att snabbt kunna återgå till normal drift om en extern leverantör drabbas.

Fråga 6:

Hur integreras dessa lärdomar i kommunens arbete med anpassningen till den nya lagen?

Svar:

Lärdomarna utgör en direkt drivkraft för vårt NIS2-implementeringsprojekt. Den nya lagen ställer specifika och skärpta krav på just säkerheten i leverantörskedjan, vilket gör att vi kan omsätta våra erfarenheter i strukturerat och lagstadgat arbete.

Exempel på integration:

- **NIS2-krav på leverantörer:** NIS2-direktivet kräver åtgärder för att säkerställa säkerheten i leverantörskedjan. Våra nya interna riktlinjer och processer för upphandling och leverantörsstyrning utformas nu för att direkt uppfylla dessa skärpta krav, såsom att ställa krav på leverantörers egen informationssäkerhetsnivå.
- **Incidentberedskap:** Erfarenheterna av incidenthantering driver utvecklingen av vår nya Incidenthanteringsprocess i enlighet med NIS2, som kräver att betydande incidenter rapporteras till relevant tillsynsmyndighet och att vi har tydliga rutiner för att hantera incidenter orsakade av leverantörer. Här har vi sett till att skapa en väg in för alla informationssäkerhetsincidenter dock behöver ytterligare arbete genomföras för att inkludera dataskyddsincidenter (GDPR).
- **Kulturell förändring:** Angreppet har lyft informationssäkerhetsfrågan till en strategisk nivå och understryker vikten av att ledningen tar sitt ansvar (också ett tydligt krav i NIS2).

Jacob Högfeldt (M)
Ordförande kommunstyrelsen



INTERPELLATION KF 2025-10-20

Ställd till KSO, Jacob Högfeldt (m)

Fråga om status för kommunens arbete med anpassning till ny cybersäkerhetslag (NIS2)

Kommunfullmäktige beslutade den 15 april 2024 (§ 51) att anta *Riktlinje för informationssäkerhet i Strängnäs kommun*. Detta beslut innebär att kommunen har åtagit sig att bedriva ett systematiskt, riskbaserat och långsiktigt arbete med informationssäkerhet i enlighet med internationella standarder och gällande lagstiftning.

Den nya cybersäkerhetslagen, som bygger på EU:s NIS2-direktiv, förväntas träda i kraft den 15 januari 2026. Lagen innebär betydligt skärpta krav på kommuner, bland annat vad gäller riskhantering, kontinuitetsplanering, incidentrapportering och tydligt ledningsansvar – det vill säga hur kommunen förebygger störningar, säkerställer att verksamheten fungerar även i kris, och rapporterar allvarliga IT-incidenter.

Ett aktuellt exempel på utmaningarna är det cyberangrepp som nyligen riktades mot systemleverantören **Miljödata**, vars tjänster används av ett stort antal kommuner i Sverige, bland annat Strängnäs kommun. Angreppet ledde till att viktiga verksamhetssystem blev otillgängliga under en längre tid och att personuppgifter riskerade att röjas. För en kommun kan det innebära att handläggning av personalärenden försenas, eller att anställdas uppgifter hamnar i orätta händer. Det som hände visar att kommuner kan drabbas hårt när viktiga system ligger hos externa leverantörer. Den nya lagen är till för att förebygga sådana problem, genom att kräva bättre kontroll, uppföljning och rapportering.

Detta är en fråga som berör alla invånare och all kommunal service, oavsett politisk inriktning. Därför är det viktigt att fullmäktige får en tydlig bild av hur Strängnäs kommun arbetar med dessa frågor.

Mot denna bakgrund vill jag ställa följande frågor till kommunstyrelsens ordförande:

1. Hur ser det aktuella läget ut i Strängnäs kommuns arbete med att anpassa sig till den kommande cybersäkerhetslagen (NIS2)?
2. Vilka konkreta åtgärder har vidtagits sedan fullmäktiges beslut den 15 april 2024 för att omsätta riktlinjerna i praktiken?



3. Hur säkerställs att alla nämnder och förvaltningar tar fram och följer lokala handlingsplaner för informationssäkerhet, i enlighet med beslutet?
4. På vilket sätt förbereder kommunen sig för att kunna uppfylla de nya lagkraven senast vid ikraftträdandet den 15 januari 2026?
5. Vilka lärdomar drar kommunen av cyberangreppet mot Miljödata när det gäller beroendet av externa leverantörer?
6. Hur integreras dessa lärdomar i kommunens arbete med anpassningen till den nya lagen?

Vänligen

Marie Ericsson Drötte

Gruppledare

Ledamot Kommunfullmäktige

Lokalt partiet