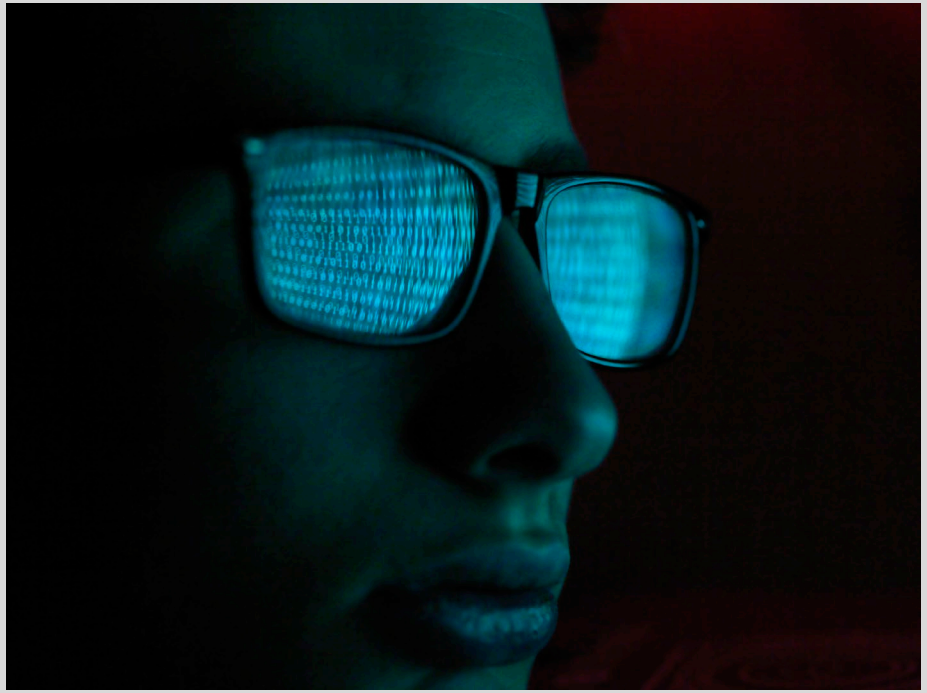
NIS2 och cybersäkerhetslagen- påverkan på våra ramavtalsupphandlingar och era framtida avrop

Tina Norelius & Matilda Thomsen
Statens inköpscentral

Bakgrund

Cyberattacker växer snabbt i omfattning, kostnader och i hur sofistikerade de är

– en av de snabbast växande formerna av brottslighet i världen



STATENS INKÖPSCENTRAL

Cyberhot

- **Terrorattacker**
  - Anlitas av andra länder eller utförs av övertygelse
  - Målet är IP, data eller att skapa kaos
- **Cyberattacker**
  - Utförs av kriminella grupper
  - Målet är pengar

Andra hot och brister

- Dåligt utvecklade tjänster
- Brister i lösning och leverans (ingen redundans)
- Bristande instruktioner och kompetens (den mänskliga faktorn)
- *Dålig koll på leverantörskedjan*
- *Bristande upphandlingsunderlag/krav*

STATENS INKÖPSCENTRAL

NIS2-direktivet

- Direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen. (Cybersäkerhet = datasäkerhet).
  - Krav på säkerhet i nätverk och informationssystem.
- Kommer genomföras i Sverige genom cybersäkerhetslagen (CSL).

CER-direktivet

- Direktiv om samhällsviktiga verksamhetsutövares motståndskraft.
- Alla samhällsviktiga verksamhetsutövare omfattas även av NIS, men inte tvärtom.
- Kommer att genomföras i Sverige genom lagen om motståndskraft hos kritiska verksamhetsutövare.

Direktiven ska införas samtidigt!

STATENS INKÖPSCENTRAL

NIS2/CSL – tillämpning

Högkritiska sektorer	Andra kritiska sektorer
☐ Energi (el*, **fjärrvärme**, olja, gas och väte) ☐ Transport (luft, tåg, vatten, väg) ☐ Bankverksamhet ☐ Finansmarknads-infrastruktur ☐ Hälso- och sjukvård (sjukhus, **EU-referenslaboratorier, Forskning och utveckling av medicin**) ☐ Dricksvatten ☐ **Avloppsvatten** ☐ Digital infrastruktur (IXP, DNS, TLD, moln, **datacenter, CDN, elektronisk kommunikation och betrodda tjänsteleverantörer**) ☐ **Offentlig förvaltning (stat, regioner och kommuner)** ☐ Förvaltning av IKT-tjänster (mellan företag) ☐ Rymden	☐ **Post- och budtjänster** ☐ **Avfallshantering** ☐ Tillverkning, produktion och distribution av kemikalier ☐ **Produktion, bearbetning och distribution av livsmedel** ☐ Tillverkning (medicintekniska produkter, datorer, elektronikvaror och optik, elapparatur, övriga maskiner, motorfordon och släpfordon, påhängsvagnar, andra transportmedel) ☐ Digitala leverantörer (sökmotorer, marknadsplatser online och **sociala nätverk**) ☐ Forskning

Fetstilade sektorer är nya i förhållande till NIS

STATENS INKÖPSCENTRAL

Undantagna från NIS2

- Regeringen, Regeringskansliet, myndigheter som lyder under Riksdagen och domstolar.
- Enskilda verksamheter som bedriver säkerhetskänslig verksamhet eller brottsbekämpning.

Oklart efter påtalande av MSB i remissrundan.

- Verksamheter som träffas av sektorsspecifik unionsrättsakt (ex. DORA)

STATENS INKÖPSCENTRAL

Största förändringarna i förhållande till NIS

- Fler omfattas
- Ensad incidentrapportering
- Kraftigare sanktioner
- Skarpare krav
- Tydligare ansvar för ledningen
- Stärkt internationellt samarbete
- Paketlösning med CER-direktivet

STATENS INKÖPSCENTRAL

Åtgärder i den egna organisationen

Analys

✓ Laginventering
✓ Risk- och sårbarhetsanalys
✓ GAP-analys

Roller & ansvar

✓ Fördela ansvar
✓ Utbilda ledning och personal
✓ Dokumentera allt

Åtgärder

✓ Identifiera åtgärder
✓ Ha en strategi (molntjänster, on-prem etc.)
✓ Skapa handlingsplan

STATENS INKÖPSCENTRAL

Minimikrav för riskhantering

1. Incidenthantering,
2. kontinuitetshantering,
3. **säkerhet i leveranskedjan,**
4. **säkerhet vid förvärv**, utveckling och underhåll av nätverks- och informationssystem …,
5. strategier och förfaranden för användning av kryptografi och kryptering

…

(3 kap. 1 § i förslaget till ny CSL)

STATENS INKÖPSCENTRAL

Specifika krav för offentliga verksamhetsutövare

- **Offentliga verksamhetsutövare** har utöver ansvaret för säkerheten i sin egen verksamhet ett ansvar för nya och befintliga leverantörer i leveranskedjan.
- Får betydelse för IT-upphandlingar.

STATENS INKÖPSCENTRAL

Säkerhetsprövning av leverantörer

- Bedöma och beakta:
  - den övergripande kvalitén och resiliensen hos produkter och tjänster.
  - de riskhanteringsåtgärder för cybersäkerhet som är inbyggda i produkterna och tjänsterna.
  - cybersäkerhetspraxis – inbegripet förfaranden för säker utveckling.
- Införliva riskhanteringsåtgärder för cybersäkerhet i avtal med sina direkta leverantörer och tjänsteleverantörer.

Skäl 85 i NIS2-direktivet

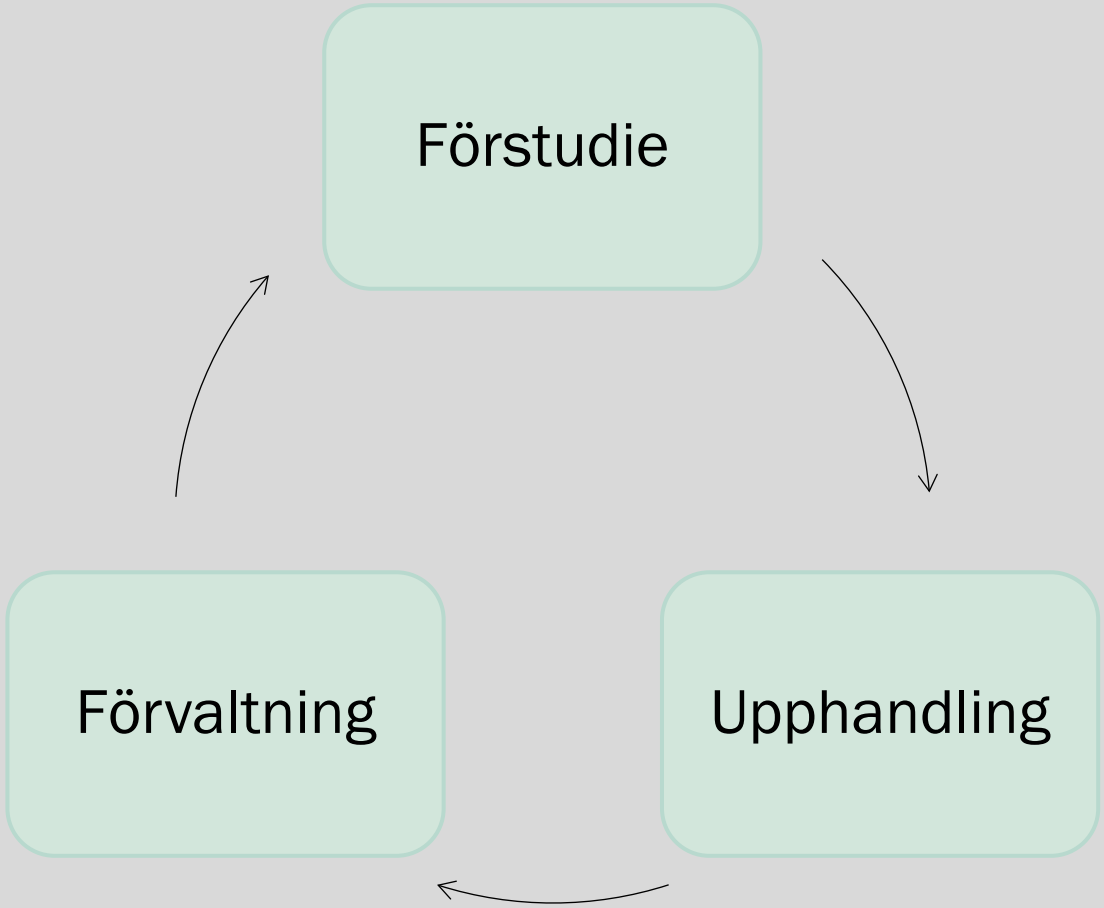
STATENS INKÖPSCENTRAL

Krav

- **Säkerhetspolicy och riskpolicy**
- **Incident- och kontinuitetshantering.**
- Certifieringar (ex. ISO 270001).
  - Cybersäkerhetscertifiering?
- SLA, Pentest (simulerad cyberattack), redundans, kryptering.
- CSOC (Cyber Security Operations Centre).
- Uppföljningsåtgärder.

STATENS INKÖPSCENTRAL

Ramavtalens kretslopp – Kammarkollegiets ”tre ben”



STATENS INKÖPSCENTRAL

Informationssäkerhet i ramavtalsprocessen

Analys

Förstudie

- Identifiera upphandlingsföremål och risker
- Förstå myndigheters behov
- Bedöma marknadens mognad

Säkerställande

Upphandling

- Krav och villkor
- Avropsform påverkar nivån för krav
- Regulatoriska krav underlättar

Slutprodukt

Förvaltning

- Uppföljning av säkerhetskrav
- Sanktioner enligt huvuddokument
- Lärdomar till nästa förstudie

STATENS INKÖPSCENTRAL

Avväganden i avrop

- Utifrån den riskanalys som har gjorts ta ställning till:
  - Vilka krav har tillvaratagits genom ramavtalet?
  - Finns möjlighet att ställa egna krav genom kravkatalog (FKU)?
  - Täcker detta in våra behov för att kunna säkerställa en god cybersäkerhetsnivå?

STATENS INKÖPSCENTRAL

Tänk slutligen på...

...att nulägesanalys, GAP-analys och åtgärder enligt NIS m.m. kan avropas från Kammarkollegiets ramavtal.

Managementtjänster – Utredning, ledning och verksamhetsutveckling (ULV).

Managementtjänster – Verksamhets- och organisationsutveckling (VU).

IT- konsulttjänster – IT-säkerhet

...att det (via MSB) finns och kommer att finnas vägledningar om hur man ska arbeta enligt NIS2.

...att det finns en frågelåda på MSB:s hemsida, NIS2-CER@msb.se

STATENS INKÖPSCENTRAL

KAMMARKOLLEGIET