Cybersäkra upphandlingar

i en allt osäkrare omvärld

Tobias Ander

SecureByMe

Tobias Ander

Senior rådgivare, Securebyme AB
Informationssäkerhet

Författare

Ordförande kommunfullmäktige

Informationssäkerhetschef i offentlig sektor

SecureByMe

Du förstör hela vårt Business case!

SecureByMe

Varför cybersäkerhet i upphandling?

- Offentlig sektor är utsatt – attacker +39% jan 2026 vs 2025; myndigheter/vård mest utsatta.
- Myndigheter hanterar enorma datavolymer och kräver hög tillgänglighet . IT-avbrott kan få effekter som ett strömavbrott.
- Orolig omvärld, offentlig tidigt drabbade i konflikter.

Säkerhetsgapet ökar varje dag

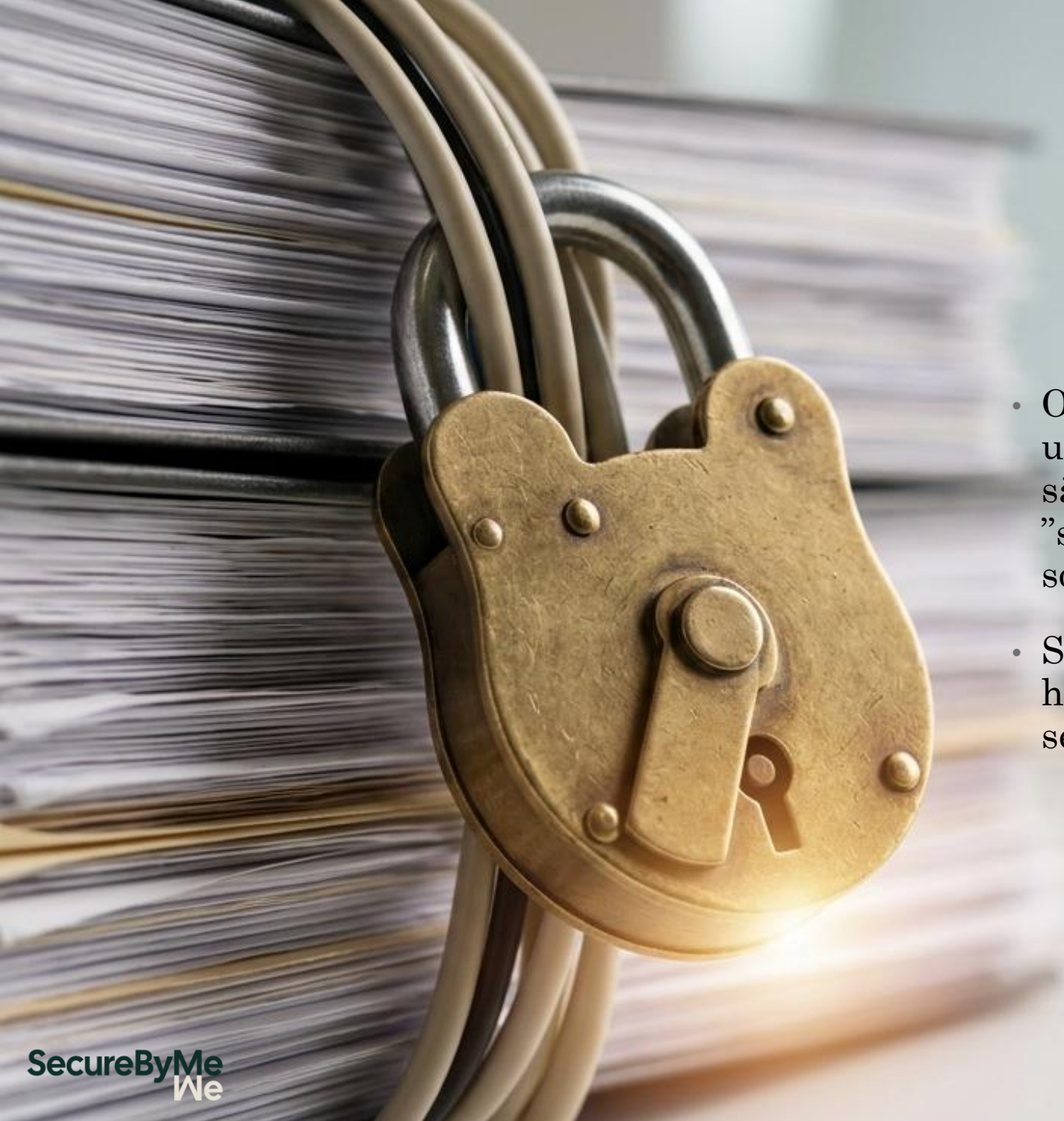
- Offentlig sektor för en orättvis kamp mot angripare.
- Digitalisering, AI.
- Klyftan mellan teknik och säkerhet växer okontrollerat utan lagstiftning.

Relevant lagstiftning

- Säkerhetsskyddslagen (för säkerhetskänsliga uppgifter).
- NIS2/Cybersäkerhetslagen (20 sektorer, nu även offentlig sektor).
- GDPR (dataskyddsförordningen) – leverantören blir oftast personuppgiftsbiträde.

NIS2: Innehåll och effekter

- NIS2 kräver bl.a. löpande riskanalys, incidenthantering, leverantörssäkerhet och ledningsinvolvering.
- Myndigheter och leverantörer inom samhällsviktiga sektorer måste införa dessa åtgärder.
- Vid upphandling kan även leverantörer tvingas följa NIS2-krav om de levererar kritiska system.



Säkerhetsskydd och sekretess

- Om upphandlingen berör säkerhetskänsliga uppgifter (t.ex. militär, polis) krävs säkerhetsskyddsavtal. Avtalen säkerställer ”samma skydd uppnås hos leverantören som hos den upphandlande organisationen”.
- Säkerhetsskyddsavtalet kan avse hemliga handlingar, känslig verksamhet (min nivå: sekretess).

SecureByMe We

GDPR och dataskydd

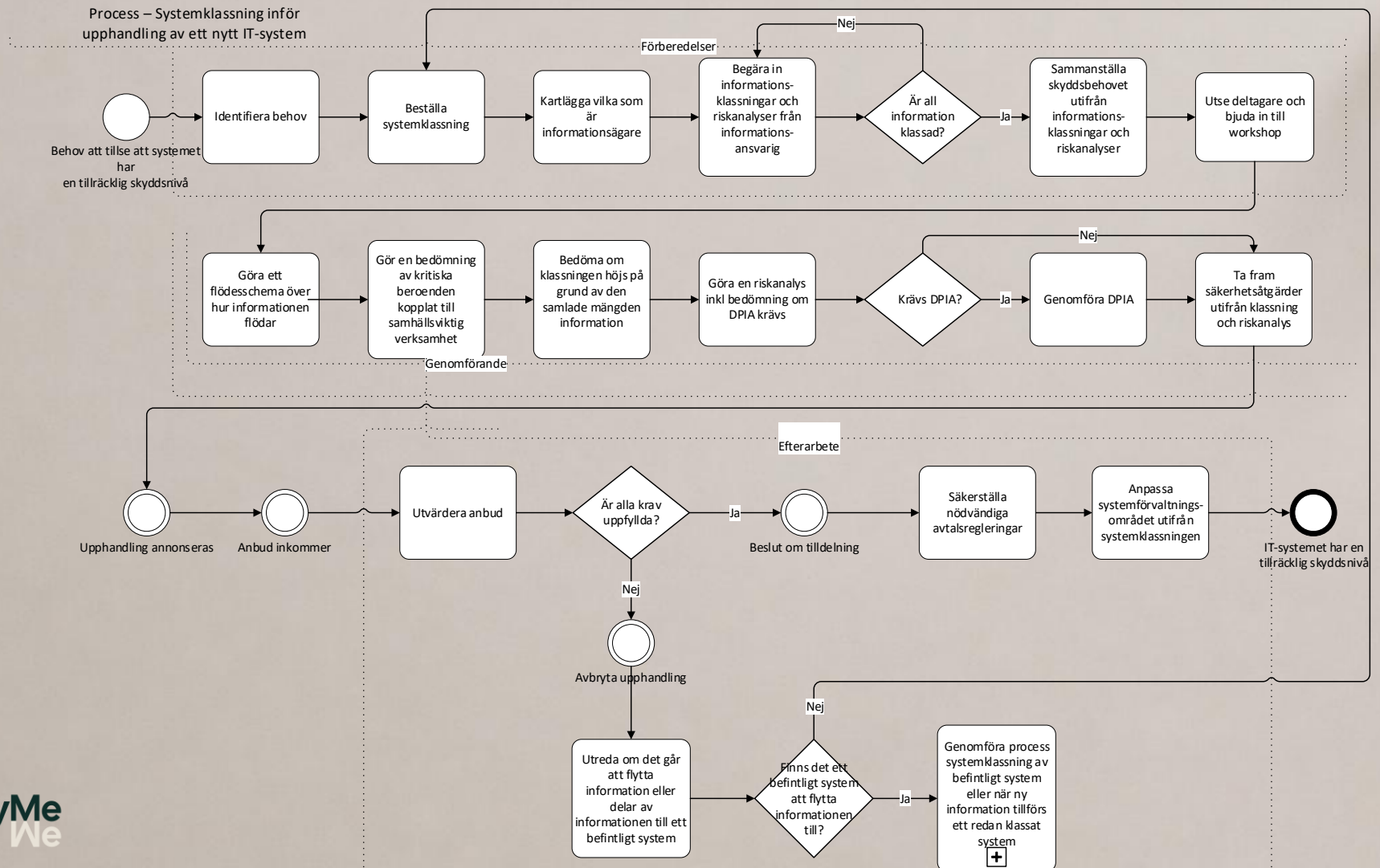
- Vid personuppgiftsbehandling i upphandling är köparen normalt personuppgiftsansvarig och leverantören personuppgiftsbiträde
- Det krävs ett biträdesavtal mellan köpare och leverantör (inkl. underleverantörer) som specificerar säkerhet och rutiner.
- Tekniska och organisatoriska åtgärder måste säkerställas (t.ex. kryptering, åtkomstkontroller) för att skydda personuppgifter.

SecureByMe

Inköpsprocessen

- Vem gör vad och när?
- Var går gränserna?
- Vem håller i helheten?

Säkerhetskrav i nya IT-system



Riskanalys och upphandlingsprocessen

- Inkludera informationsklassning och riskbedömning tidigt i upphandlingen
- Integrera säkerhetskrav i varje steg: kravspecifikation, anbudsvärdering, kontrakt, uppföljning.
- Använd checklistor (exempel finns hos Tobias) för att ställa frågor om leverantörenssäkerhetsnivå (t.ex. krav på certifieringar, backup, loggning, incidenthantering)

Ställa krav på informationssäkerhet

- Parkeringsautomater
- Städtjänster
- Resebyrå
- Grävarbete i stads-gata
- Upphandlingsplattform
- IT-system

Leverantörskedja och underleverantörer

- Kräv transparens om underleverantörer. Se över att leverantörer inte i sin tur har outsourcat kritiska delar utan er vetskap.
- Formalisera att alla underleverantörer omfattas av samma avtal och säkerhetskrav (t.ex. genom att krav på kedjan ingår i avtalsvillkoren).
- Identifiera väsentliga leverantörsberoenden i förväg – t.ex. där viktig data kan lagras "var som helst i världen".

Säkerhet i molntjänster

- Vid molntjänst/outsourcing behövs detaljerade avtal: dataägaransvar, datalagringsplatser, åtkomstkontroller och särskilda säkerhetsåtgärder
- Ex. *Avtala exakta IT-säkerhetsåtgärder (regelbundna backup-tester, skydd mot skadlig kod, DDoS-skydd, incidentövningar)*

Autentisering och behörigheter

- Kräv multifaktorautentisering (MFA) för administrativa konton och fjärråtkomst. Begränsa leverantörens behörigheter strikt.
- Använd minst rollbaserad åtkomstkontroll och dokumentera åtkomstgrupper, se checklistfrågor om behörighet och loggning

Loggning och spårbarhet

- Tjänsten/systemet ska ha loggning av alla relevanta händelser (inloggningar, åtkomst till känsliga uppgifter, ändringar).
- Formulera krav på SIEM eller centraliserad logghantering, inklusive lagringstid och årlig granskning av loggar.

Informationssäkerhet, kryptering

- Alla känsliga uppgifter ska vara krypterade i vila och vid överföring. Använd erkända algoritmer och hantera nycklar säkert
- Ex.*”All överförd känslig information skall skyddas med stark kryptering (minst AES-256). Data i vila ska lagras krypterat, och krypteringsnycklar ska hanteras av en oberoende nyckelhanterare*”.

Incidenthantering och rapportering

- Leverantören ska ha dokumenterade rutiner för incidenthantering och omedelbart rapportera alla incidenter som kan påverka beställarens data eller tjänster.
- Ex. *”Leverantören skall skriftligen rapportera säkerhetsincidenter utan dröjsmål, och beskriva åtgärder som vidtagits.”*

Sårbarhetshantering

- Kräv att leverantören aktivt söker efter och åtgärdar säkerhetssårbarheter i sina system
- Ex. *”Leverantören ska ha rutiner för hantering av sårbarheter i IT-miljön (patchhantering, penetrationstester etc.)”*

SecureByMe

Systemarkitektur och åtkomstkontroll

- Fråga om systemets arkitektur: segmentering, DMZ, brandväggar, redundans och molnbaserade lösningar.
- Dokumentera krav på isolering av känsliga system och minimera attackytan.

Avtalspunkter och garantier

- Inkludera krav på certifieringar (t.ex. ISO/IEC 27001 eller branschspecifika standarder) för leverantören eller systemet.
- Specificera möjligheter att genomföra oberoende revisioner eller penetrationstester av systemet, samt ta ut vite vid avtalade brister.

Uppföljning och kontinuerlig övervakning

- Planera regelbundna avstämningar och granskningar: Leverantören ska lämna dokumentation över incidenter, revisioner och statusrapporter.
- Tydliggör ansvar: vem gör vad vid hantering/utredning av incidenter, vem har åtkomst till leverantörens loggar.

Vanliga fallgropar

- Otydliga eller för få krav
- Otydlighet i leverantörskedjan
- Ingen kontinuerlig kontroll

Fallgropar (forts) och motåtgärder

- Överkrav kontra rörliga mål – Att skriva för många detaljer om teknisk implementation kan hämma flexibilitet
- Otillräcklig kompetens – För hög teknisk nivå för inköparen att hantera
- Brist på sanktioner – Om ingen sanktion finns är kraven tandlösa

Verktyg och mallar

- MSB:s vägledningar och checklistor för informationssäker upphandling
- DIGG:s rekommendationer för upphandling av data , Datainspektionens och SKR:s guider om dataskydd, Kammarkollegiets ramavtalsmallar (Avropa.se) och best practice.
- Systematisk Informationssäkerhet (Ander & Hofsten) 2025.

Miljödata-attacken

- **Bakgrund:** Aug 2025 hackades IT-leverantören Miljödata. ”200 kommuner och regioner påverkades”, ~1,5 miljoner personuppgifter läckte
- **Konsekvenser:** Delar av personal- och journalsystem låg nere i dagar/veckor. Risk för identitetsstöld och förtroendeskada uppstod
- **Lärdomar:** Säkerställ leverantörens redundans och separering av kunddata; avtala expresskrav på data-säkerhet (MFA, segmentering, kryptering). Krisplaner och incidentträning för att snabbt agera i leverantörsincidenter.

Tietoevry-ransomware

- **Bakgrund:** Jan 2024 utsattes Tietoevry (stor it-leverantör för offentlig sektor) för en ransomware-attack . Detta påverkade bl.a. Tandvårds- och läkemedelsförmånsverket (TLV) och flera regioner.
- **Konsekvenser:** Flera system (bl.a. TLV:s läkemedelsdatabas) låg nere i månader; en rapport uppskattade TLV:s driftkostnader till över 110 Mkr . Regioner tvingades övergå till manuella rutiner tills service återställdes.
- **Lärdomar:** Klara SLA:er för återställning (t.ex. backup-test och återläsningstid) ; tydligt ansvar i avtal om driftsäkerhet. Flera drabbade organisationer krävde skadestånd från leverantören, vilket belyser vikten av skadeståndsklausuler.

Kalix-kommun

- **Bakgrund:** Dec 2021 utsattes Kalix kommun för en omfattande ransomware-attack. I princip alla system låstes och krävde lösen.
- **Konsekvenser:** Lönesystem, journaler mm utsattes. Personalen övergick till manuella rutiner i veckor . Attacken blev en väckarklocka i Sverige.
- **Återhämtning:** Kalix valde att inte betala och återställde med hjälp av säkrade backups (hackarna hade inte nått dessa) .
- **Lärdomar:** Investera i segmentering, 2FA och utbildning – efter attacken införde kommunen bland annat multifaktor och ny nätverksarkitektur .

Sammanfattning av fallstudier

- Exempel visar att brister hos leverantörer kan skapa relativt stora störningar
- Gemensamma lärdomar: backup och kontinuitet är kritiska, tydliga krav på säkerhetsnivå, incidentstyrning och redundans behövs. Ställa krav och följa upp dem.

Avslutningsvis

- Ha koll på vilken information som kommer hanteras direkt och indirekt av leverantör. Tag hjälp av säkerhetsorganisationen.
- Uppföljning, uppföljning, uppföljning!
- En god säkerhetskultur är grunden.

Tack!
Tillsammans gör vi skillnad!

SecureByMe

Tobias Ander

tobias@securebyme.se

+46 70 33 71 433

securebyme.se

/in/tobiasander