Trygg och säker informationshantering

Lanseringsseminarium 2023-09-27

OFFENTLIGA FASTIGHETER

Lanseringsseminarium 2023-09-27

Medverkande:

- Lars Lidén, huvudförfattare, erkänd inom fastighetsbranschen för sin expertis inom området informationshantering i förvaltning och projekt, senior projektledare, Meta Fastighetsadministration AB
- Thomas Nilsson, huvudförfattare, beskriver sig själv som en pragmatisk säkerhetsnörd med snart 40 års arbete inom informations- och cybersäkerhet. En av grundarna av Certezza AB.
- Bo Baudin, strateg mjuk digital infrastruktur, SKR

Lanseringsseminarium om skriften Trygga säkra informationsmiljöer - ur ett fastighetsperspektiv

Under lanseringsseminariet presenteras resultaten från samarbetet Offentliga fastigheters projekt Trygga säkra informationsmiljöer – ur ett fastighetsperspektiv.

Datum: 27 september 2023

Tid: 8.00 – 9.30

Plats: Digitalt

Kostnad: Kostnadsfritt

Sista anmälningsdag: 26 september 2023

OFFENTLIGA FASTIGHETER

Program

1. Inledning – Bo Baudin
2. Övrigt material inom området – Thomas Nilsson och Lars Lidén
3. Trygga och säkra informationsmiljöer – Thomas Nilsson och Lars Lidén
4. Summering och avslut – Bo Baudin

Övrigt material inom området

- → KLASSA – Grundvärdering och minimikrav (länk)
- → Vägledning för molntjänster (länk)
- → Konsumtion av e-legitimationer (länk)
- → Bildanalys – referenskonsekvensbedömning (länk)
- → KLASSA för IoT tillsammans med RISE (länk)
- → Informationssäkerhet inom fastighetsområdet & IoT (länk)
- → Vägledning för IoT-tjänster – från behov till realisering (länk)
- → Informationssäkerhet i fastighetsorganisationen (länk)
- → Boverkets utredning kring OVK och sensorteknik

OFFENTLIGA FASTIGHETER

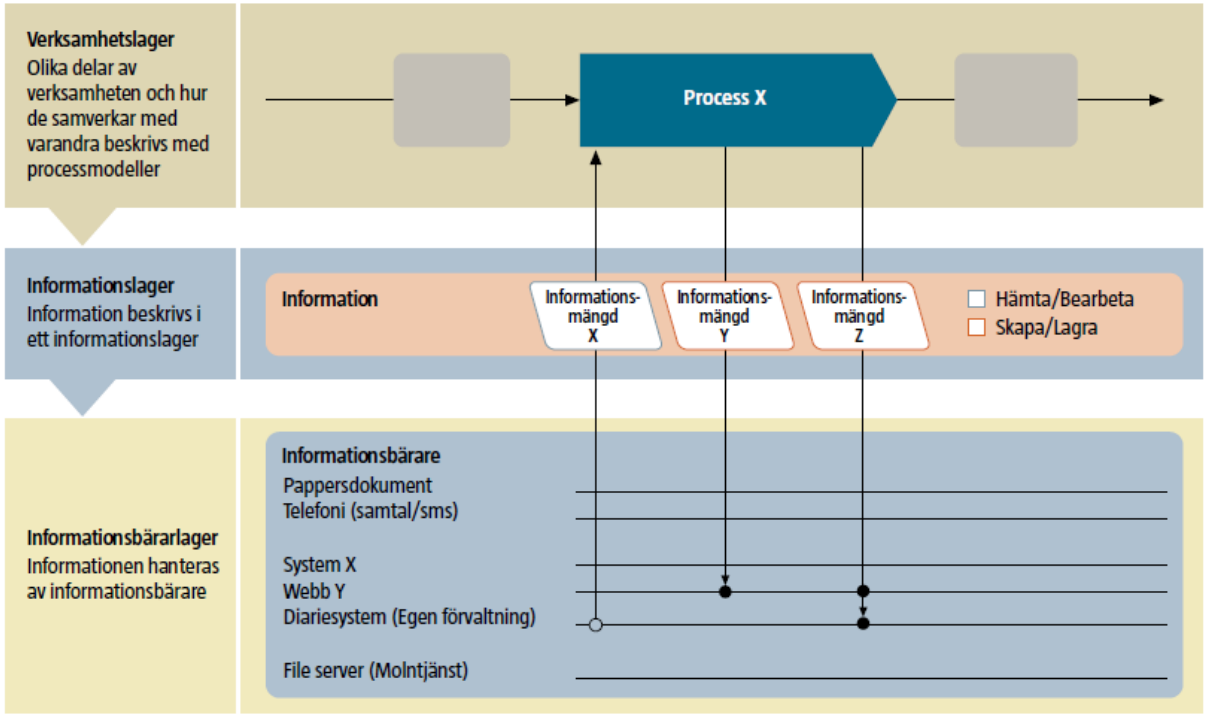
Informationssäkerhet i fastighetsorganisationen

- Processorienterad informationskartläggning
- Informationsägandet
- Informationsklassning
- Skyddsåtgärder

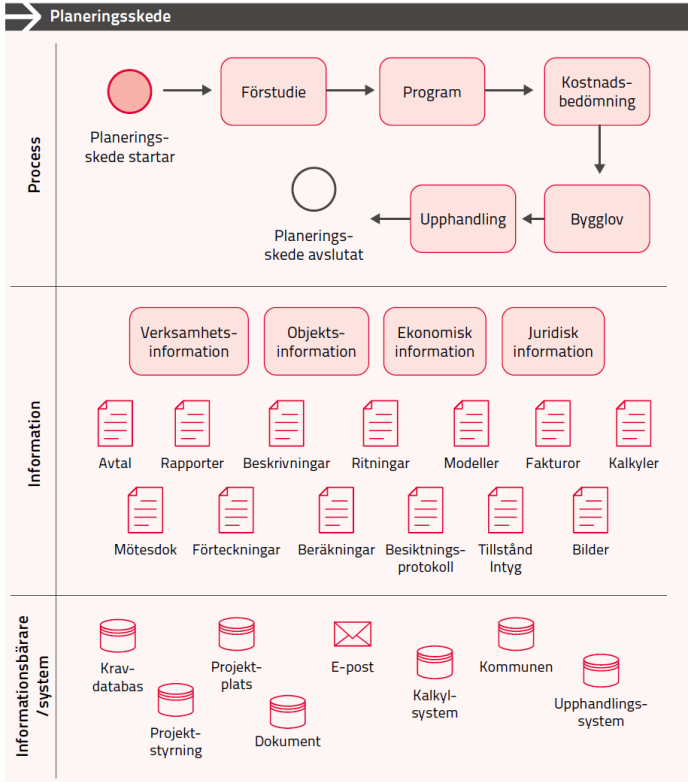
Processorienterad informationskartläggning

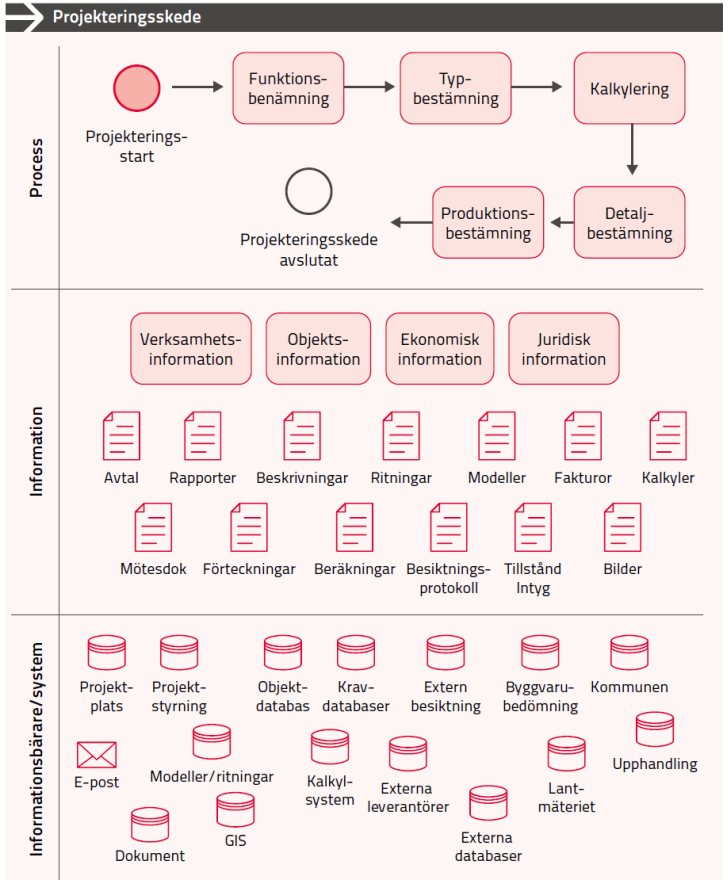
MSB – Vägledning för processorienterad informationskartläggning

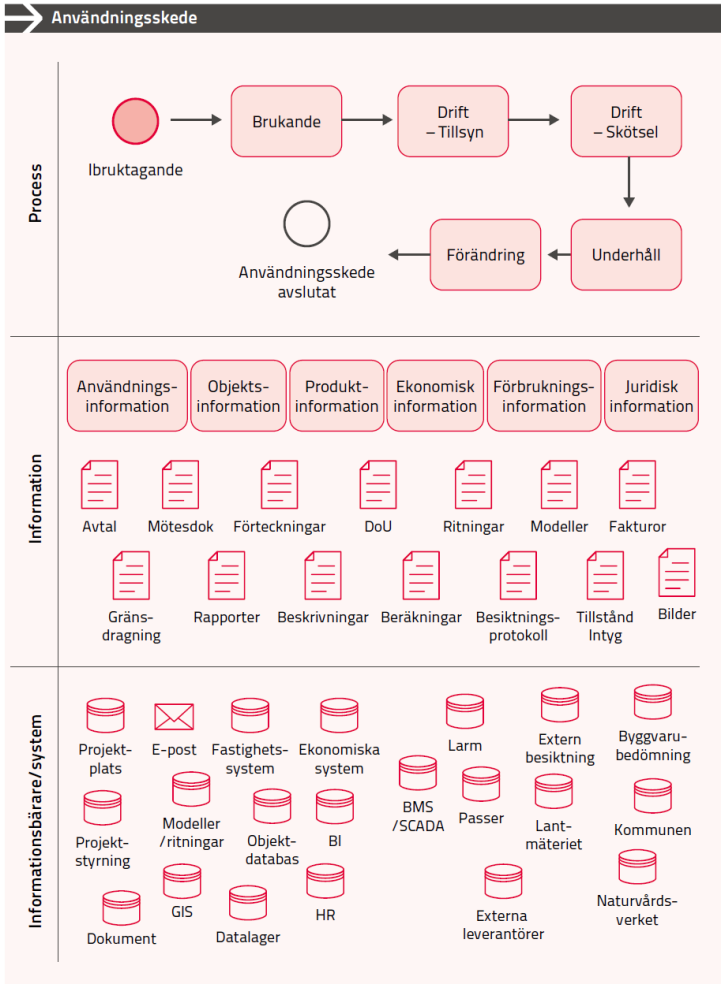
- Identifiera processer
- Identifiera information
- Identifiera bärare/system



Processorienterad informationskartläggning



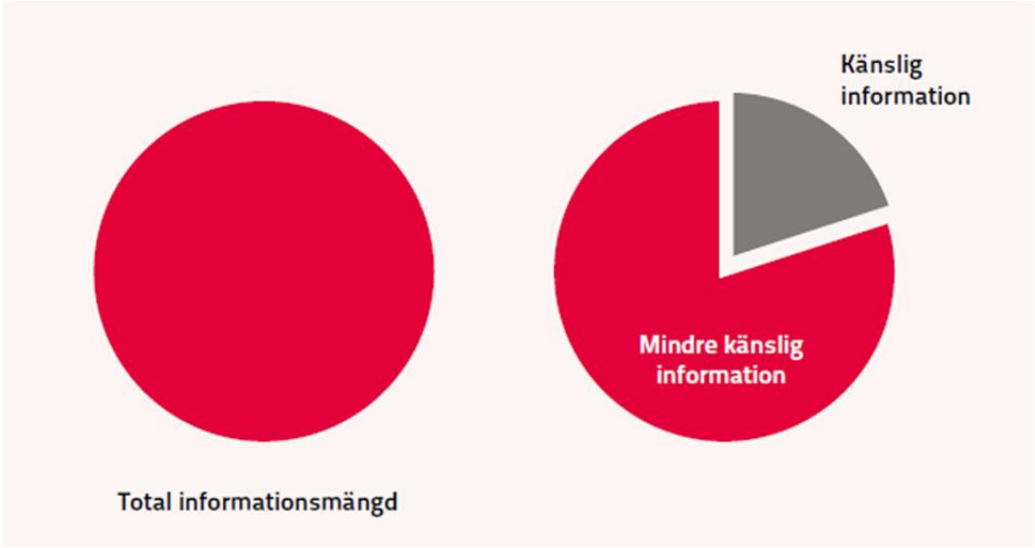




OFFENTLIGA FASTIGHETER

Informationsklassning

- **Konfidentialitet**
  - Vad blir skadan om information hamnar i orätta händer?
- **Riktighet**
  - Vad blir skadan om information inte är korrekt?
- **Tillgänglighet**
  - Vad blir skadan om information inte är tillgänglig?



Informationsklassning - exempel

Tekniska system

Information	Konfidentialitet	Riktighet	Tillgänglighet	Kommentar
Mark och grund	1	1	1	
Väggar	1–3	1	1	
Bjälklag	1–3	1	1	
Yttertak	1–3	1	1	
Gas och luft	2	2	2	
Vatten och vätska	2	2	2	
Avlopp och avfall	1	1	1	
Kyla och värme	2	2	2	
Luftbehandling	2	2	2	
Elkraft	2–3	2–3	2	
Belysning och dagsljus	1	1	1	
Automation	2–3	2–3	2	
Information och kommunikation	2–3	2	2	
Transport	1	1	1	
Säkerhet och skydd (larm)	3	3	3	
Utrustning	0	0	0	

Utrymmen

Information	Konfidentialitet	Riktighet	Tillgänglighet	Kommentar
ID	0	1–2	1	
Benämning	0–3	1–2	1	Beror på rum
Area	0	2	1	
Dimensionerande värden	0–2	0–3	0–3	Beror på rum
Skydd	2–3	2–3	1–3	Beror på rum
Säkerhetsklass	3–4	2–3	1–2	
Hygienklass	1	3	0–2	Verksamhet
Material – ytskikt	0–1	1	0–1	
Försörjning	3–4	3–4	3–4	

OFFENTLIGA FASTIGHETER

Trygg och säker informationshantering

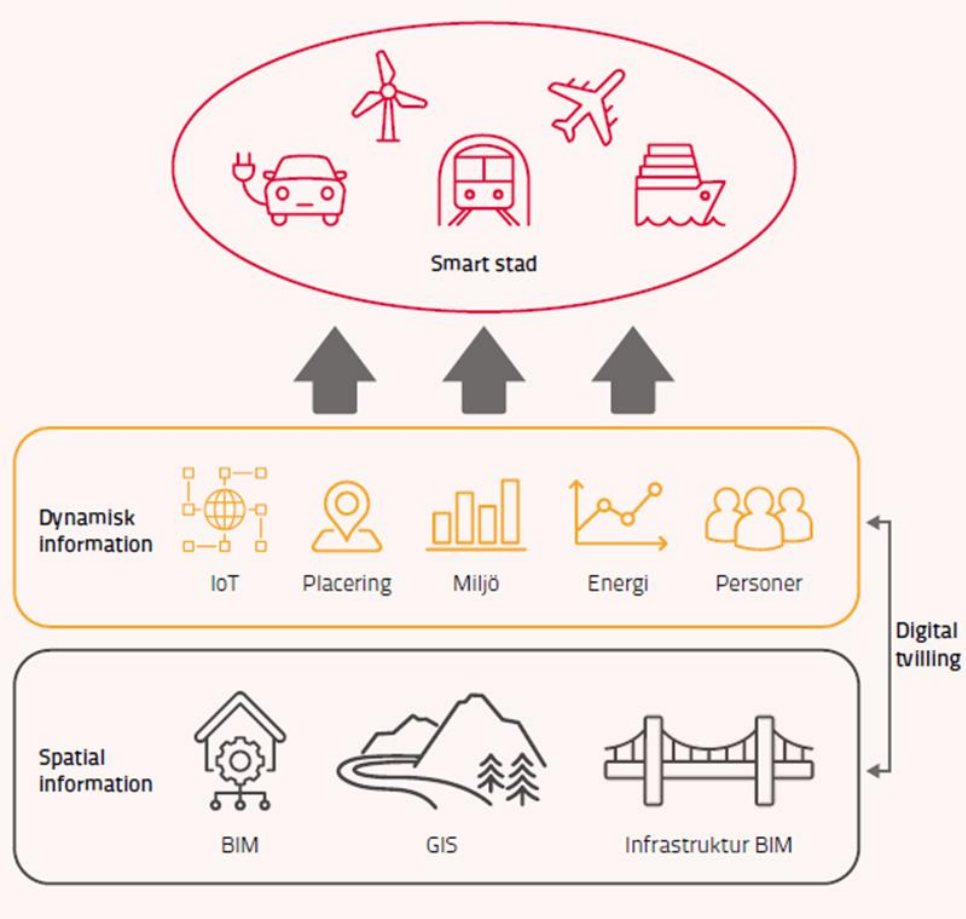
- Redogörelse för regulatoriska krav
  - Säkerhetsskydd
  - CER-direktivet
    - Åtgärder för att stärka motståndskraften i viss samhällsviktig verksamhet
  - NIS2-direktivet
    - Säkerhet i nätverk och informationssystem för samhällsviktiga tjänster
- Vägledning i säkerhetskyddsanalys
- Beskrivning av risk och riskanalys
- Vägledning i tillämpat systematiskt riskanalysarbete
- Praktiska exempel

OFFENTLIGA FASTIGHETER

Syfte och målgrupp

- Att informera och orientera offentliga fastighetsägare i förhållningssättet till säkerhetsskyddslagen och de nyligen beslutade EU-direktiven NIS2 och CER.
- Att tillhandahålla en beskrivning och en vägledning i systematiskt riskhanteringsarbete.
- Att belysa konkreta exempel kring hantering av automatiserade byggnader avseende:
  - Analysobjekt och skyddsvärden
  - Hot och hothändelser
  - Sårbarheter
  - Konsekvenser
- Primär målgrupp är personer verksamma i fastighets- och säkerhetsorganisationer inom offentlig sektor.
- Sekundär målgrupp är konsulter och leverantörer som verkar inom fastighetsbranschen.

Bakgrund - Ökad digitalisering



Våra byggnader blir allt mer smarta och den byggda miljön spelar också en viktig roll i den smarta staden där allt fler funktioner samverkar.

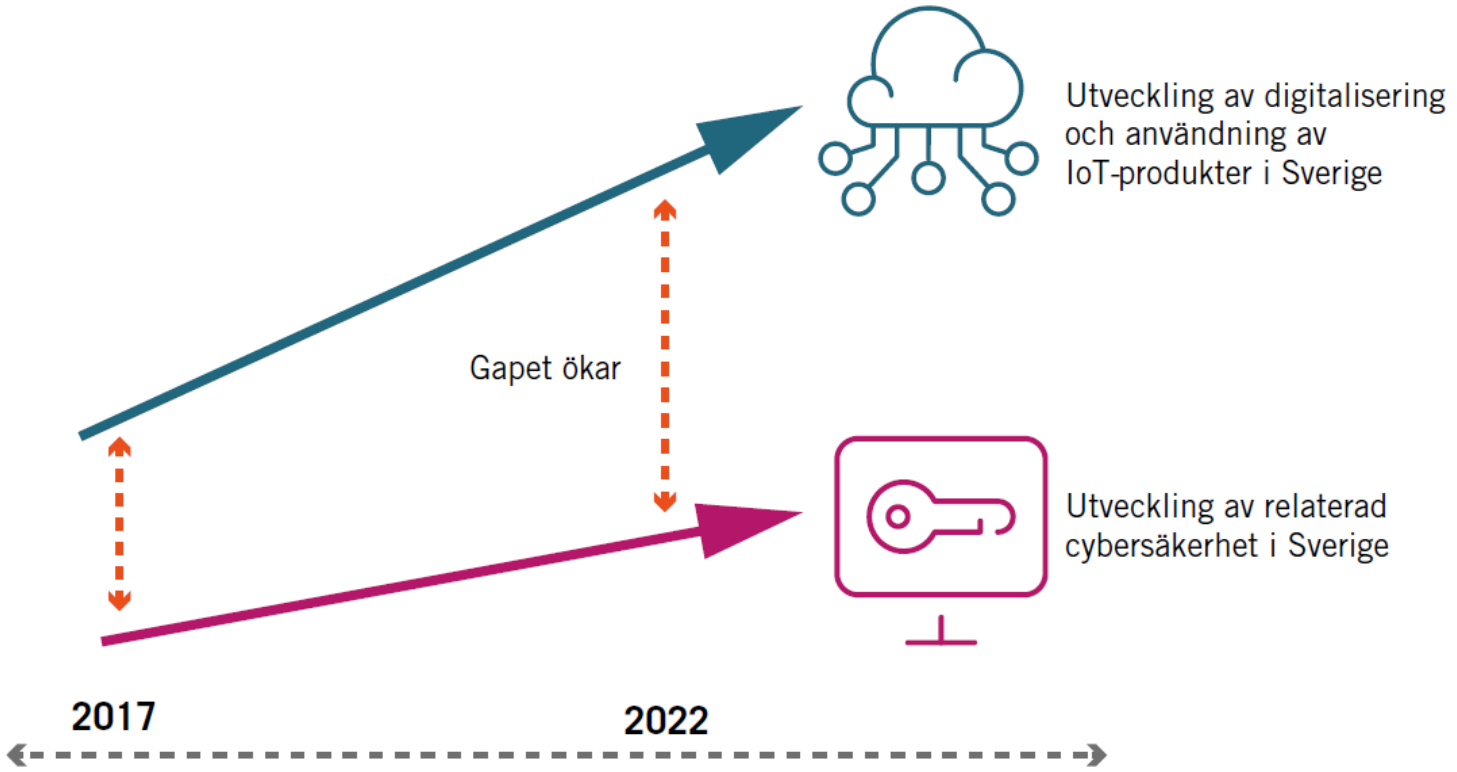
Den smarta staden ställer krav på bland annat tillgång till data.

Både personer och organisationer måste vara beredda att dela med sig av information.

Att avgöra vilken data vi är beredda att dela med oss av bottnar i kunskap och analyser av vilken data vi hanterar och hur våra byggnader är uppbyggda.

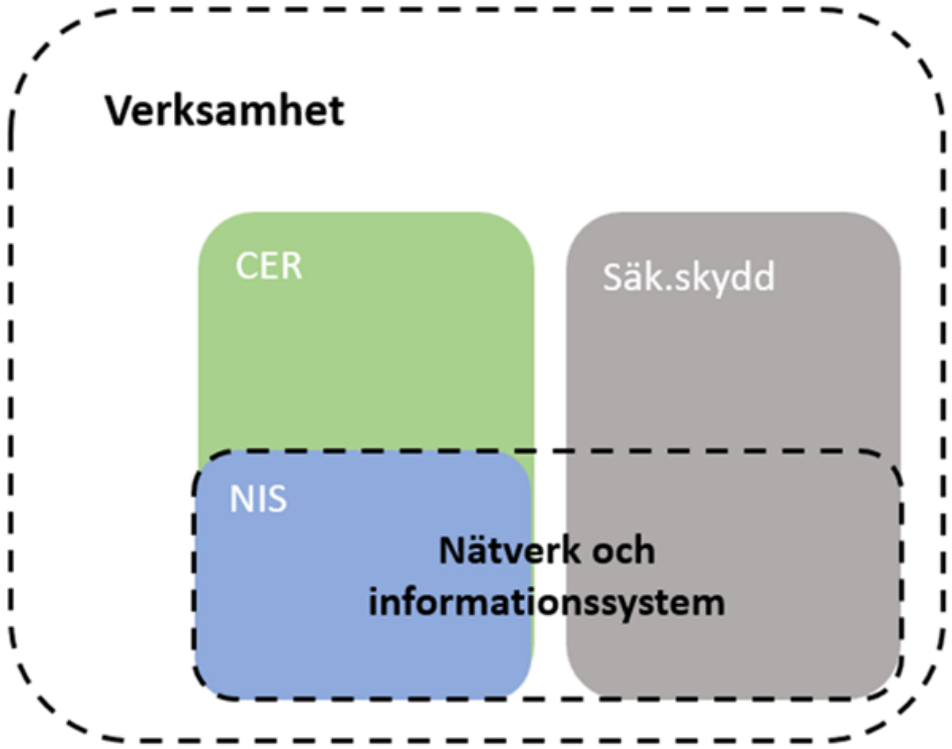
OFFENTLIGA FASTIGHETER

Bakgrund - Digitalisering och informationssäkerhet i otakt



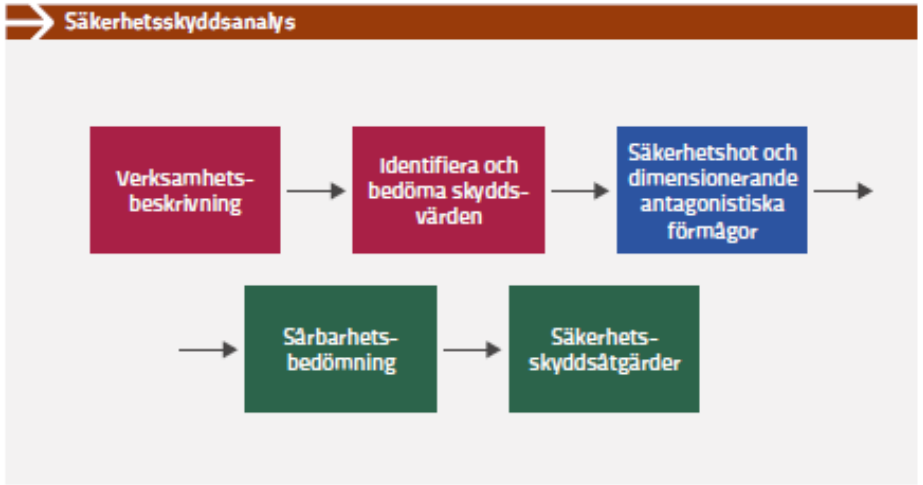
Olika regleringar att förhålla sig till

- Säkerhetsskyddslagen är överordnad NIS.
- Säkerhetsskyddslagen innebär att OSL även tillämpas av privata företag.
- CER- och NIS2-direktivens exakta förhållande till svensk lagstiftning är under utredning.
- CER-direktivet behandlar allt kontinuitetsarbete för samhällskritiska verksamheter medan NIS/NIS2-direktiven inriktar sig mot de it-miljöer som dessa verksamheter är beroende av.



Säkerhetsskyddslagen – vem träffas?

- Träffas av lagen gör verksamhet som antingen:
  - Bedriver säkerhetskänslig verksamhet
  - Hanterar säkerhetsskyddsklassificerade uppgifter
- Antagonistiska hot i fokus!
  - Hotaktör som har förmåga och avsikt att skada som kan leda till konsekvenser för Sveriges säkerhet.
- Första steget är en säkerhetsskyddsanalys:
  - Vad ska skyddas?
  - Mot vad ska det skyddas?
  - Hur ska det skyddas?



OFFENTLIGA FASTIGHETER

Säkerhetsskyddslagen - påverkan

VILKEN SPECIFIK PÅVERKAN HAR SÄKERHETS-SKYDDSLAGEN PÅ FASTIGHETSFÖRVALTARE?

Som fastighetsförvaltare är det bra att känna till hur krav på säkerhets-skydd påverkar utformningen av lokaler och hur information som kan kopplas till lokaler, hyresgäster och rörelsemönster behöver hanteras.

Med en förståelse för säkerhetsskydd kan samarbete underlättas med aktörer som bedriver säkerhetskänslig verksamhet, till exempel i de fall en säkerhetsskyddad upphandling behövs och utpekade lokaler på för-hand kan göras redo för att möjliggöra anpassning till säkerhetsskydd.

Exempel: Några exempel på byggnader och lokaler som kan bli föremål för säkerhetsskydd är lokaler för förvaring av säkerhetsskyddsklassifi-cerade uppgifter, lokaler där samhällsviktig verksamhet bedrivs samt lokaler som är utpekade ledningsplatser för kris- och krigsledning.

OFFENTLIGA FASTIGHETER

Säkerhetsskyddsanalys – att tänka på

- **Vår organisation?** Om det inte tydligt om säkerhetskänslig verksamhet bedrivs kan metoden för säkerhetsskyddsanalys användas i syfte att bedöma om så är fallet.
- **Säkerställ kompetens!**
- **Säkerställ förutsättningar.** För att genomföra analysen kan behövas lämpliga rum och förvaringsutrymmen, rutiner och säkerhetsskyddsavtal eller säkerhetsskyddsöverenskommelser (B/H).
- **Förankra.** Intern förankring hos verksamhetens ledning är nödvändig genom hela processen för att säkerställa stöd och resurser.
- **Processtegen i metodiken är en vägledning**. Det praktiska genomförandet av en säkerhetsskyddsanalys är inte så sekventiellt som metoden visar utan arbetet i de olika stegen sker ofta parallellt.
- **En säkerhetsskyddsanalys är ett omfattande åtagande**. Den ställer höga krav på organisationen. Framför allt krävs:
  - God kännedom om verksamheten
  - God förmåga att identifiera skyddsvärden i förhållande till Sveriges säkerhet
  - God förmåga att identifiera antagonistiska hot i relation till identifierade skyddsvärden
  - God förmåga att identifiera sårbarheter för skyddsvärdena

CER-direktivet – viktiga samhällsfunktioner

Förmåga att upprätthålla viktiga samhällsfunktioner inom:

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvård
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Offentlig förvaltning
- Rymden
- Produktion, bearbetning och distribution av livsmedel

VILKEN SPECIFIK PÅVERKAN HAR CER-DIREKTIVET PÅ FASTIGHETSFÖRVALTARE?

Fastighetsförvaltning är inte en verksamhet som leder till att direkt omfattas av kraven i CER-direktivet. Eventuell omfattning av direktivet kan däremot komma från sekundära håll och beroenden.

Exempel: Hyresgäster som bedriver verksamheter inom sektorerna som listas ovan kan exempelvis komma att ha särskilda behov som att anläggningen eller byggnaden de hyr på olika sätt behöver anpassas för att de ska kunna efterleva kraven i regleringen. Sådana krav på säkerhetsåtgärder bör ställas av hyresgästerna i upphandlingsskedet men kan även tillkomma vid avtalsförnyelse.

På samma sätt kan fastighetsägare komma att påverkas indirekt genom att deras samverkanspartners i närliggande branscher, som exempelvis tillhandahåller eldistribution, dricksvatten och avloppsvattenhantering, träffas av regleringen. Det kan leda till ökade samarbets- och leveranskostnader för fastighetsägarna.

OFFENTLIGA FASTIGHETER

NIS2 – nätverks- och informationssystem

Säkerställa tillförlitligheten och säkerheten hos samhällsviktiga nätverks- och informationssystem/tjänster för:

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvård
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Förvaltning av it-tjänster
- Offentlig förvaltning
- Rymden
- Post- och budtjänster
- Avfallshantering
- Tillverkningsindustri
- Digitala leverantörer
- Forskning

VILKEN SPECIFIK PÅVERKAN HAR NIS 2-DIREKTIVET PÅ FASTIGHETSFÖRVALTARE?

När det kommer till fastighetsbranschen så omfattas man inte, precis som i fallet för CER-direktivet, direkt av kraven för NIS 2. Eventuell omfattning av direktivet kan kommer i så fall även här från sekundära håll och beroenden.

Exempel: Krav som kommer från fastighetsägarnas hyresgäster på säkerhetsåtgärder för att skydda deras it-miljö. Dessa krav bör ställas av hyresgästerna själva i upphandlingsskedet eller vid avtalsförnyelse. Säkerhetsåtgärderna bör syfta till att reducera verkningar av sådana konsekvenser som hyresgästerna identifierat i de riskanalyser som NIS 2-direktivet kräver.

På samma sätt kan fastighetsägare komma att påverkas indirekt genom att deras samverkanspartners i närliggande branscher, som tillhandahåller exempelvis eldistribution, fjärrvärme eller avlopps- och avfallshantering, träffas av regleringen. Det skulle kunna leda till ökade samarbets- och leveranskostnader för fastighetsägarna.

OFFENTLIGA FASTIGHETER

CER och NIS – att tänka på

- Identifiera berörd verksamhet som leverantör av samhällsviktig tjänst och anmäla detta till aktuell tillsynsmyndighet.
- Identifiera vilka delar av verksamheten som bedriver samhällsviktiga tjänster samt, exakt vilka beroenden som dessa verksamhetsdelar har i form av nätverk och informationssystem (i fallet för NIS) samt alla andra former av beroenden inklusive personalsäkerhetsfrågor (i fallet för CER).
- Bedriv riskanalysarbete för samtliga risker som kan drabba den samhällsviktiga verksamheten och vidta nödvändiga åtgärder.
  - Här ska samtliga risker beaktas för att möta CER-direktivet och specifikt de risker som kan drabba de kritiska it-miljöerna för att möta NIS-/NIS2-direktiven.
- Säkerställ tillräckliga säkerhetsåtgärder.
  - De beslutade åtgärderna får inte understiga de specifika krav som återfinns i MSB:s och tillsynsmyndigheternas föreskrifter.
- Säkerställ att organisationen har tillräckligt effektiva processer och rutiner för att förhindra och upptäcka, rapportera, hantera, återhämta sig från och utvärdera incidenter.
- Bygg en organisation för, och öva kontinuitet. Att planera och träna för tänkbara avbrott i den samhällsviktiga leveransen är vitalt för att kunna absorbera, anpassa sig till och återhämta sig från incidenter.
- Bedriv regelbunden uppföljning för att uppnå ständiga förbättringar som en del av systematiken.

Exempel på skyddsvärden och analysobjekt

- Olika tekniska system med sensorer sitter på en stor mängd data som är användbar ur diverse olika perspektiv. Dels ur drift- och förvaltningsperspektiv, dels som enskild byggnad, dels som del i ett fastighetsbestånd eller stad i vilket man kan samköra data och dela system och därmed få bättre överblick och en effektivare skötsel.
- Ett antal system kan vara skyddsvärda och en analys av respektive systemen behöver göras för att bedöma hot, sårbarhet och konsekvens av en eventuell händelse.

Exempel på skyddsvärden och analysobjekt

Analysobjekt	Exempel	Potentiell sårbarhet för cyberhot
Mark och utemiljö	Mark	-
	Parkeringstjänster	Ja
	Karttjänster	Ja
Byggnadskonstruktion	Stomme	-
	Skalskydd	-
Lokaler	Planlösning	Ja
	Lokalanvändning	Ja
	Karttjänster	Ja
Gas och luftsystem	Medicinska gaser	Ja
	Tryckluft	-
Vattensystem	Rent vatten	Ja
Avlopp och avfallssystem	Avlopp	Ja
	Avfall	-
Kyla och värmesystem	Kyla	Ja
	Värme	Ja
Luftbehandlingssystem	Luftkvalitet	Ja
Elkraftssystem	Normalkraft	Ja
	Reservkraft	Ja
	Avbrottsfri kraft	Ja
Automationssystem	Övervakning	Ja
	Styrning	Ja
Informations- och kommunikationssystem	Positionering	Ja
	Kommunikation	Ja
Transportsystem	Hissar, rulltrappor	Ja
	Lyftar	Ja
Säkerhets- och skyddssystem	Passagesystem	Ja
	Brandlarm, utrymningslarm	Ja
Belysning och dagsljus	Belysningsstyrning	Ja

OFFENTLIGA FASTIGHETER

Exempel på hot och hothändelser

- Obehörig åtkomst till data, vilket kan exponera känslig information och kränka integritet.
- Manipulation av funktion, vilket kan störa rutiner och påverka verksamheten.
- Sabotage eller skadegörelse, vilket kan störa kritiska processer och tvinga verksamheten att avbryta sin verksamhet.
- Ransomware-attacker, vilket kan leda till driftsstörningar för verksamheten.
- DDoS-attacker som överbelastar kommunikationssystem och orsakar driftsstörningar.
- Insiderhot, där personal eller externa entreprenörer med tillgång till olika system kan använda sin åtkomst för att orsaka skada, stjäla information eller manipulera system.
- Katastrofer och klimatpåverkan – extremväder som skyfall och hårda vindar kan medföra översvämningar, jordskred med mera.
- Brand orsakad av tekniska fel alternativt orsakad av människor, oavsiktligt eller avsiktligt

Exempel på sårbarheter

- Otillräcklig kontroll och övervakning av åtkomst till styrningssystem, vilket kan leda till obehörig användning och potentiell skada för verksamheten.
- Sårbarheter i trådlös kommunikation, vilket kan leda till att kryptering bryts och känslig information avlyssnas.
- Svagheter i fysisk säkerhet, såsom otillräckligt skyddade styrsystem eller dörrar, vilket kan ge obehöriga personer åtkomst till känsliga områden.
- Brister i återställningsplaner för att hantera säkerhetsincidenter, vilket kan förlänga återhämtningstiden och förvärra konsekvenserna för verksamheten.
- Otillräckliga säkerhetsåtgärder för att skydda data som är lagrad i molnet, vilket kan leda till dataintrång och exponering av känslig information.
- Brister i leverantörs- och underentreprenörsledet, vilket innebär att komponenter eller tjänster kan ha säkerhetsbrister som påverkar hela systemet.

Exempel på konsekvenser

- Driftstörningar och stillestånd på grund av bristande funktionalitet.
- Juridiska och ekonomiska konsekvenser på grund av överträdelser av lagar och regler kring informationssäkerhet och personsekretess.
- Skadat rykte och förtroende hos allmänhet och andra intressenter.
- Förlust av data vilket kan försvåra drift, planering och felsökning, och resultera i längre driftstörningar.

OFFENTLIGA FASTIGHETER

Risk, riskhantering och riskanalys

Ett systematiskt riskarbete innebär att:

1) **Identifiera och värda hot**.
2) **Formulera risker**.
3) **Bedöma risker**.
4) **Behandla risker**, exempelvis genom att vidta riskreducerande åtgärder.
5) **Följa upp riskåtgärder** för implementation och effektivitet.

Riskanalys - exempel

Exempel på bedömning av sannolikhet för hothändelser inom analysobjektet Luftbehandling.

Hot-händelse ID	Hothändelse (aktör+ev intention+agerande)	Sannolikhet intervall (drop-down)	Mest troligt sannolikhet (ggr per år)	Motivering sannolikhet
H-001	tekniker anger felaktiga styrvärden för ventilation	>1 & ≤10 ggr/år (Måttlig)	2	Bedömning görs sett till tidigare historik från incidenter och störningar. Bedömningen är relativt säker.
H-002	tekniker medvetet anger felaktiga styrvärden för ventilation	<0,1 & ≤1 ggr/år (Låg)	0,3	Bedömning görs sett till stor andel leverantörer och tidigare händelser i omvärlden. Bedömningen är relativt osäker.
H-003	ransomware gör att styrning av ventilation inte är möjlig	<0,1 ≤1 ggr/år (Låg)	0,4	Bedömning görs sett till tidigare händelser i branchen och i omvärlden. Bedömningen är relativt osäker.
H-004	sensordata för luftkvalitet kommer inte fram till styrsystemet	>1 ≤10 ggr/år (Måttlig)	6	Bedömning görs sett till tidigare historik från incidenter och störningar. Bedömningen är relativt säker.

Hothändelserna från föregående figur har här försetts med sannolikhetsbedömningar vilka dessutom motiveras/beskrivs.

OFFENTLIGA FASTIGHETER

Kommande och pågående arbeten

- → Vägledningsarbete pågår på många håll och inom många områden
  - → Internationellt, EU, nationellt, sektorsvis…
  - → Risk för motsägelsefull vägledning ökar med många aktörer och stor risk för desinformation
- → Ytterligare reglering inom informations- och cybersäkerhet
  - → EU, nationellt, sektorsvis…
  - → EU är ganska konsekvent ☺ Systematiska informationssäkerhetsarbete!
- → Behov av en nationell haverikommission
  - → Lära av egna och andras incidenter
  - → Vem tar lead?
- → Förfinade och förbättrade metodik och våga bli konkret
  - → KLASSA har banat väg i form av att bli konkret
  - → Nytt Vinnova-finansierat projekt tar sikte på förfinad metodik och förbättrade kravkataloger
- → Informations- och cybersäkerhet måste bli en del av den vanliga vardagen!

OFFENTLIGA FASTIGHETER

Trygg och säker informationshantering

OFFENTLIGA
FASTIGHETER