INFORMATIONSSÄKERHET

Aktivt säkerhetsskydds-arbete krävs av fler aktörer inom samhällsbyggnad

Vad har hänt i närtid?

- Antalet verksamhetsutövare och personer som deltar i säkerhetskänslig verksamhet ökar, bland annat genom uppbyggnaden av totalförsvaret och Sveriges Nato-inträde. Därmed omfattas allt fler av krav på säkerhetsprövning och säkerhetsskydd.
- NIS2-direktivet implementeras i svensk lagstiftning under 2025 och omfattar nu fler samhällsbyggnadsaktörer än tidigare, inklusive leverantörer och underkonsulter som hanterar kritiska funktioner.
- Cyberattacker mot svenska organisationer ökade med 20% i oktober 2025 jämfört med samma månad året innan. Angreppen riktas allt oftare mot verksamheter med kritiska system och dataflöden, vilket gör samhällsbyggnadssektorn särskilt utsatt när digitalisering och uppkopplade lösningar ökar.
- AI och automatisering skapar nya möjligheter men även nya risker – från dataläckor till manipulerade beslutsunderlag. Frågan om digital tillit växer snabbt i betydelse.

Joakim Håhl
CDO/CIO & Säkerhetschef

Expert på IT-strategi, digital transformation och säkerhet. Driver innovation och effektivisering med fokus på verksamhetsanpassade IT-system, säker datahantering och robusta säkerhetsstrategier.

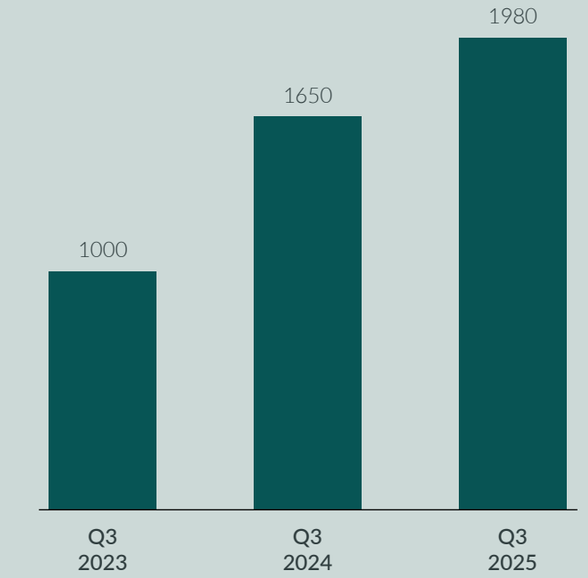
Samhällsbyggnadssektorn befinner sig i ett nytt säkerhetslandskap, där allt fler delar av samhället omfattas av ökade krav på beredskap och resiliens. Utvecklingen ställer för många aktörer krav på såväl IT-säkerhet och motståndskraft mot påverkansförsök som utökat arbete med säker informationshantering. För allt fler aktörer behöver arbetet bli en integrerad del av verksamhetsstyrning och kultur – det blir en förutsättning för långsiktigt förtroende och fortsatt funktion trots ökad risk för störningar.

Arbete med säkerhet, informationsskydd och resiliens har gått från att vara en nischad expertfråga till att beröra allt fler. Under 2025 har flera aktörer uttryckt sig publikt kring sin bild av läget. Exempelvis tecknar MSB:s nationella risk- och sårbarhetsbedömning och Säkerhetspolisens lägesbild 2024-2025 en gemensam bild av ett hybridhot, där sårbarheter i samhället testas och där både offentliga och privata aktörer påverkas. Fler attacker sker med samhälle och infrastruktur som mål. Påverkansförsök riktas nu i högre grad än tidigare mot exempelvis energibranschen, transportsektorn, kommuner, fastighetsägare och konsultbolag. I takt med att omvärldsläget blir allvarligare får beredskapsarbetet ytterligare fokus. Ett exempel på skärpt inriktning är att Myndigheten för Samhällsskydd och Beredskap (MSB) byter namn till Myndigheten för Civilt Försvar från och med 1 januari 2026.

> ”
>
> Säkerhet handlar inte bara om att skydda system – utan om att bygga förtroende och förmåga. För oss är det en strategisk fråga som måste vara integrerad i affärsplanering, styrning och riskhantering – inte något som läggs på i efterhand. När vi ser säkerhet som en investering i resiliens stärker vi både leveransförmåga, förtroende och konkurrenskraft över tid. De organisationer som tidigt väver in säkerhets- och beredskapsfrågor i sina beslut kommer också att stå starkare när regelverk skärps och omvärlden förändras snabbt.
>
> **Joakim Håhl, CIO/CDO & Säkerhetschef Hifab**

Cyberattacker mot svenska organisationer ökar

Genomsnittligt antal cyberattacker per organisation och vecka i Sverige



Källa: Check Point Research via Dagens Infrastruktur, 29 okt 2024.

I och med uppbyggnaden av totalförsvaret och Sveriges Nato-inträde ökar antalet verksamhetsutövare och personer som deltar i säkerhetskänslig verksamhet, även inom civila delar av sektorn. Allt fler konsulter, tekniska förvaltare och entreprenörer omfattas av krav på säkerhetsprövning och säkerhetsskyddsavtal. Detta syns bland annat i att antalet registerkontroller som SÄPO genomför ökar kraftigt.

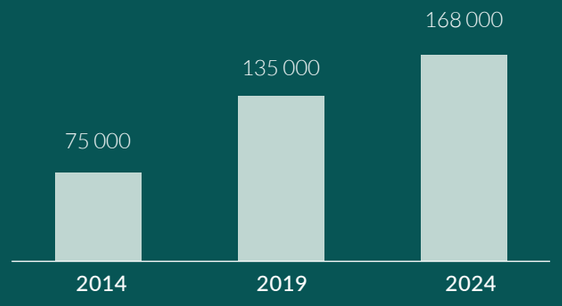
Samtidigt blir den digitala miljön alltmer avancerad och intrång sker inte bara via hackade system, utan genom att nyttja social manipulation, otillräcklig åtkomstkontroll eller att rutiner glöms bort i vardagen.

Samhällsbyggnadssektorn behöver gemensamt öka sin förmåga att både hålla kritiska system igång och se till att känslig information inte hamnar i orätta händer. De nya regelverken, som NIS2 och uppdaterade krav inom säkerhetsskydd, gör att fler aktörer nu behöver bygga strukturer för riskanalys, incidentrapportering och kontroll. Det är tydligt att teknik inte räcker – det är människor, kultur och samverkan som avgör hur robust en organisation verkligen är.

För att hantera skyddsvärd information eller viktig infrastruktur krävs att hela kedjan, från ledning till leverantör, följer samma principer. Fler aktörer i samhällsbyggnadssektorn behöver bygga en högre förmåga att skydda viktiga verksamheter, upprätthålla drift även under störningar och agera ansvarsfullt i en komplex riskmiljö. De företag som lyckas bygga en stark säkerhetskultur, där medvetenhet, rutiner och samverkan är en del av vardagen, blir också mer resilienta mot såväl tekniska angrepp som mänskliga misstag.

Mer än dubbelt så många registerkontroller

Antalet registerkontroller som Säkerhetspolisen genomfört på begäran av arbetsgivare (både offentliga och privata). Registerkontroller är en del av säkerhetsprövning för att bedriva säkerhetskänslig verksamhet.



Källa: Säkerhetspolisens lägesbild 2024/2025.

Nyckelfrågor för beslutsfattare inom fastighet & samhällsbyggnad

1.

Har vi en uppdaterad strategi för att hantera de krav som följer av NIS2 och säkerhetsskyddslagstiftningen?

2.

Hur arbetar vi med att identifiera och skydda vår mest skyddsvärda information och infrastruktur?

3.

Finns det en tydlig ansvarsfördelning och kultur som stödjer säkerhetsmedvetet agerande i vardagen?

4.

Hur ser vi till att leverantörer och samarbetspartners uppfyller samma säkerhetskrav som vi själva?

5.

Har vi övat på att hantera en cyberincident eller informationsläcka och vet vi vem som gör vad?

6.

Ser vi säkerhetsarbetet som en kostnad eller som en investering i långsiktig resiliens och förtroende?