LÖNSAM SÄKERHET

METODBOK

Klas Nilsson

Lönsam säkerhet

Metodbok

av

Klas Nilsson, CPP, PCI, PSP, CFE, CISM

Upphovsrättsinnehavare 2026 © Klas Nilsson

Mångfaldigande av innehållet i denna bok, helt eller delvis, är enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk förbjudet utan medgivande från författarna. Förbudet gäller tryckning, kopiering, skanning, bandinspelning med mera samt lagring på datamedia.

www.securitymanager.se

info@securitymanager.se
Författare: Klas Nilsson
Redigering: Klas Nilsson
Omslag: Klas Nilsson
Vissa bilder är AI-genererade,
andra är köpta från Shutterstock
ISBN: 978-91-981320-2-1

Innehållsförteckning

Prolog 7
Introduktion 11
- Säkerhetsrelaterade kostnader 12
- Skyddskostnad och skadekostnad 12
- Säkerhetsrelaterade intäkter 13
- Överdrivna skyddsåtgärder 14
- Kompensatoriska skyddsåtgärder 16
- Optimala skyddsåtgärder 17
- Sambanden mellan centrala områden 18

Tillgångar 27
- Varför tillgångar är utgångspunkten för lönsam säkerhet 27
- Metodisk arbetsordning 28
- Att sätta ett monetärt värde på tillgångar 34
- Befintliga skyddsåtgärder 35

Hotbild 39
- Hotbild är inte en lista på hot 39
- Nulägesbild – hur hot har manifesterats hittills 40
- Från beskrivande till prediktiv analys 46
- Incidentrapportering och budgetering av skadekostnader 48

Konsekvens 53
- Konsekvens – från hot till skadekostnad 53
- Konsekvens och återhämtningsförmåga 58

Metod 71
- Tillgångar och deras egenskaper 72
- Överväganden vid val av metod 75

Organisation 85
- Organisation i en föränderlig omvärld 86
- Organisationens tre ingångsvärden 88
- Ledarstilar och deras betydelse för säkerhetsarbetet 91
- Förmågeutveckling – från plan till resultat 93
- Organisationens mognad och säkerhetskultur 95
- Kriskommunikation som organisatorisk förmåga 97

Effektivitet 103
- Funktion eller prestation 104
- Principer för ett effektivt skydd 106
- Principer för effektiv kontinuitet 109

Investering 117
- Två grundläggande kostnadstyper 118
- Att räkna – utan att fastna i matematik 120

Lönsamhet 127
- Vad menas med lönsamhet i säkerhetsarbete? 127
- Skyddskostnaden – vad kostar säkerhet egentligen? 129
- Optimal säkerhet – inte maximal 135

Mätetal 141
Varför mätetal behövs i säkerhetsarbete 141
Lönsam säkerhet i accelerationen 157
När tid blir affärens hårdvaluta 157
Beslutsnivå – när säkerhet blir styrning, inte teknik 159
Riskacceptans – när att avstå blir en strategisk kompetens 160
Förändringstakt – när världen går i flera tempon samtidigt 161
Ordlista 167
Modellens tillämpningsområde 187
Register 190
Epilog 195
Om författaren 197

Om du kunde, skulle du välja bort säkerhetsarbetet?

Prolog

Alla verksamheter har säkerhetsrelaterade kostnader. Antingen betalar man för skydd i form av personal, lås, larm och arbetstid eller så betalar man för bristande skydd genom skador, avbrott, sanktionsavgifter och förluster. Det är fullt möjligt att uppfylla fastställda krav och till och med optimera enskilda skyddsåtgärder och ändå ha höga säkerhetsrelaterade kostnader. Först när säkerhetsarbetet utgår från verksamhetens risker och affärsmål blir det möjligt att styra mot en bättre totalekonomi, där skyddskostnaden faktiskt minskar skadekostnaden mer än den själv kostar.

När jag började arbeta med säkerhet i början av 1990-talet handlade det mest om att uppfylla försäkringskrav och branschkrav. Säkerhet sågs då som en nödvändig särkostnad, något som behövde finnas för att kunna göra affärer, men som inte förväntades skapa värde. Sedan förändrades förutsättningarna. Ny teknik skruvade upp utvecklingstakten och nya hotbilder gjorde konsekvenserna både större och mer komplexa. Det som tidigare kunde hanteras med fasta krav och etablerade lösningar började kräva ett annat sätt att tänka.

Det var år 2003, när jag började studera för personcertifieringen CPP, som jag fick upp ögonen för något avgörande: säkerhet kan, i mycket större utsträckning, utformas utifrån riskanalyser och ekonomisk hållbarhet. Det ledde till att jag började utveckla en metod för att göra säkerhetsarbetet mer styrbart och mer affärsnära. Den största utmaningen har inte varit att skapa lönsamhet i säkerhetsarbetet, utan att övertyga ledningen om att det är möjligt.

Åren 2010–2012 skrev jag Säkerhetsboken 2.0 och året efter Säkerhetsboken 3.0. Då kom delar av resonemanget på pränt. År 2013 tog modellen för lönsam säkerhet sin form, ungefär som den ser ut i skrivande stund och jag började skriva den här boken. Manuset har fått växa fram långsamt, parallellt med praktik och erfarenhet, där verkliga händelser har tvingat fram precision i både begrepp och samband. Resultatet är den här boken, nästan fjorton år senare.

Lönsam säkerhet är ingen motsättning. Det är ett medvetet val.

Är säkerhet en kostnad –
eller en dold tillgång?

Introduktion

Säkerhet kostar pengar. Det är allmänt känt. Det som däremot fortfarande är oklart i många verksamheter är vad säkerhetsarbetet faktiskt kan bidra med.

I många styrelserum betraktas säkerhet fortfarande som ett nödvändigt ont. En kostnad som måste bäras för att uppfylla lagkrav, försäkringsvillkor eller för att undvika rubriker i media. Säkerhetsbudgeten ses som en försäkringspremie som man hoppas slippa använda, men som ändå måste betalas. När tiderna blir tuffare är säkerhet därför ofta ett av de områdena som ifrågasätts, reduceras eller skjuts på framtiden.

Samtidigt lever vi i en tid där hotbilden är mer komplex, mer föränderlig och mer verksamhetskritisk än någonsin tidigare.

- Cyberangrepp kan slå ut hela verksamheter över en natt.
- Leverantörsstörningar kan stoppa produktion i flera led.
- Informationsläckor kan rasera förtroende som tagit decennier att bygga upp.

Ett enda allvarligt avbrott kan få konsekvenser långt bortom den direkta skadan, i form av uteblivna intäkter, skadade relationer, juridiska påföljder och långvarig osäkerhet i organisationen.

Trots detta saknas det ofta ett gemensamt språk mellan säkerhetsfunktionen och verksamhetsledningen. Säkerhet talar risker, hot och sårbarheter. Ledningen talar lönsamhet, tillväxt, effektivitet och affärsmål. När dessa perspektiv inte möts uppstår ett glapp. I det glappet förlorar säkerhetsarbetet både genomslag och legitimitet. Det är detta glapp som den här boken syftar till att minska.

Tänk om säkerhetsarbetet inte bara sågs som en kostnad, utan som ett medel för att skydda intäkter, minska totala kostnader och skapa förutsättningar för affärer som annars inte hade varit möjliga.

Det är här begreppet **lönsam säkerhet** tar sin utgångspunkt.

Lönsam säkerhet handlar inte om att maximera skydd eller minimera kostnader, utan om att optimera sambandet mellan verksamhetens tillgångar, hotbild, konsekvenser och valda åtgärder. Det handlar om att vidta rätt åtgärd, vid rätt tidpunkt, på rätt nivå och att kunna visa vilken effekt det faktiskt ger.

För att lyckas med detta krävs ett annat sätt att tänka kring säkerhet. Ett sätt som kopplar säkerhetsarbete till organisation, investeringar, effektivitet och i slutänden lönsamhet. Det är denna helhetssyn som introduceras i detta kapitel och som resten av boken steg för steg fördjupar.

Säkerhetsrelaterade kostnader

Alla verksamheter har säkerhetsrelaterade kostnader, det vill säga kostnader kopplade till säkerhet, oavsett vilka åtgärder som vidtas eller inte. Det är viktigt att förstå att detta inkluderar både kostnader för att skapa god säkerhet och konsekvenserna av säkerhetsbrister, snarare än bara direkta kostnader för skyddsåtgärder.

En bra jämförelse är personalrelaterade kostnader, som uppstår i flera steg: vid rekrytering (exempelvis rekryteringsprocesser och introduktionsutbildningar), under anställning (lön, utbildningar, administration) och vid avslut (förlorade intäkter, nyrekrytering). På samma sätt kan säkerhetsrelaterade kostnader delas upp i olika kategorier och kontexter, inklusive ineffektiva eller överdimensionerade skyddsåtgärder samt konsekvenser av uteblivet skydd.

Verksamheten kan även ha skyddsåtgärder som inte är ändamålsenliga. Det vill säga inte verksamma mot hotbilden på grund av att de är feldimensionerade, exempelvis för svaga och skadan inträffar i alla fall eller för kraftiga och kostar onödigt mycket eller helt felaktiga för den aktuella hotbilden. Likaså kan det finnas skyddsåtgärder som inte längre behövs på grund av förändrade omvärldsfaktorer eller verksamhetsförändringar. Skyddsåtgärder kan föråldras av slitage, bristande underhåll eller andra omständigheter som gör att de inte längre är effektiva.

Skyddskostnad och skadekostnad

För att uppnå lönsamhet i säkerhetsarbetet behöver man förstå vad som påverkar kostnaderna. Dessa kan delas in i tre huvudkategorier:

- **Skyddskostnad:** Utgifter för åtgärder som förbättrar säkerheten, beroende av valda lösningar och organisationens effektivitet.
- **Skadekostnad:** Kostnader som uppstår när tillgångar skadas på grund av säkerhetsbrister – dvs. avsaknad av lämpligt skydd.
- **Juridiska påföljder:** Sanktionsavgifter, viten, böter och skadestånd vid bristande regelefterlevnad – betraktas här som en typ av skadekostnad.

Reaktivt säkerhetsarbete, dvs. att man agerar först efter en incident, gör att kostnaderna kan skena iväg jämfört med proaktivt arbete. Reaktivitet leder ofta till:

- **Svårare skada**, på grund av avsaknad av tillräckliga skyddsåtgärder.
- **Akuta** och dyrare **insatser** ofta med extern hjälp.
- **Driftstopp** och förlorade intäkter.
- **Förtroendeförlust** och förlorade kunder.

Säkerhetsrelaterade intäkter

Säkerhetsarbete kan också vara en stark värdeskapare. Genom att arbeta strukturerat med skydd, riskhantering och säkerhetskultur kan verksamheter skapa intäkter, affärsfördelar och stärkt konkurrenskraft. Här är några exempel på hur säkerhet kan bidra till ökad lönsamhet:

- **Nya affärsmöjligheter:** Säkerhetscertifieringar, regelefterlevnad och strukturerat riskarbete gör det lättare att vinna affärer, särskilt hos kunder som ställer krav på informationssäkerhet, kontinuitet eller fysisk säkerhet. ISO 22301, ISO 27001, ISO 28000 och SSF 1101 är exempel på sådant som ökar tilliten.
- **Nya marknader:** Organisationer med god riskhanteringsförmåga kan göra säkrare affärer i osäkra marknader, geografiskt eller branschmässigt, vilket möjliggör affärer där andra aktörer tvekar.
- **Bättre beslutsunderlag:** Säkerhet handlar om att undanröja risk och skapa visshet. Riskanalyser, händelsedata och strukturerade rutiner ger ledningen bättre information för att styra verksamheten framåt, med färre överraskningar och bättre precision.
- **Operativ effektivitet:** Säkerhet skapar ordning och tydlighet i processer, rutiner, instruktioner och tekniska lösningar, vilket minskar fel, avbrott och ineffektivitet. Det höjer produktiviteten och främjar ett mer proaktivt arbete.
- **God säkerhetskultur:** En trygg och välorganiserad arbetsmiljö stärker medarbetares engagemang, lojalitet och stolthet. Det gör det lättare att behålla och attrahera kompetens, vilket i sin tur stärker verksamhetens långsiktiga stabilitet.
- **Sänkta försäkringskostnader:** Ett dokumenterat säkerhetsarbete sänker riskprofilen, vilket kan ge lägre premier, självrisker och bättre försäkringsvillkor. Detta innebär en direkt ekonomisk besparing.
- **Färre kostsamma incidenter:** Förebyggande säkerhet minskar risken för driftstopp, dataintrång, juridiska sanktioner och skadestånd. Att inget oönskat händer till följd av fungerande skydd är ett affärsvärde i sig.
- **Differentiering och kvalitetsintryck:** Ett väl fungerande säkerhetsarbete är också en symbol för kvalitet, ansvar och professionalism. Det kan användas i marknadsföring, anbud och kommunikation för att stärka varumärket.

Ett genomtänkt säkerhetsarbete bidrar till ökade intäkter, minskade kostnader, ökad stabilitet och bättre beslutsfattande. Det är inte en kostnadspost utan en investering i förtroende, effektivitet och affärsutveckling.

Överdrivna skyddsåtgärder

Överdrivna skyddsåtgärder kännetecknas av att skyddskostnaderna är höga samtidigt som den faktiska minskningen av skadekostnaderna är liten eller obefintlig. I dessa fall har säkerhetsarbetet passerat den punkt där ytterligare skydd ger proportionerlig nytta. Skyddet kan upplevas som omfattande och robust, men leder i praktiken till ökande totalkostnader och försämrad lönsamhet.

Till skillnad från kompensatoriska skyddsåtgärder, där skyddskostnader och skadekostnader tar ut varandra så att totalkostnaden förblir oförändrad, innebär överdrivna skyddsåtgärder att skyddskostnaderna ökar snabbare än skadekostnaderna minskar. Säkerhetsarbetet blir därmed direkt kostnadsdrivande.

Ett vanligt sätt som överdrivet skydd uppstår på är genom felriktade skyddsåtgärder. Organisationen investerar i avancerade, tekniskt sofistikerade eller kostsamma lösningar utan tydlig koppling till den faktiska hotbilden. Skyddet dimensioneras för scenarier med låg sannolikhet eller begränsad konsekvens, medan mer sannolika och vardagliga risker inte adresseras i motsvarande utsträckning. Resultatet blir höga investerings- och driftskostnader med begränsad effekt på de skador som faktiskt inträffar.

Överdrivet skydd uppstår också ofta när verksamheten förändras över tid, men skyddsnivåerna inte omprövas. Skydd som en gång var rationellt i en riskfylld miljö kan bli kvar trots att hotbilden minskat eller förändrats. Ett exempel är verksamheter som tidigare haft särskilt skyddsvärd produktion eller funktion, men som senare ändrat inriktning. Om kostsamma tekniska skydd, bevakning och administrativa krav behålls oförändrade, uppstår ett permanent överdimensionerat skydd som inte längre står i proportion till den aktuella risken.

Ett närliggande exempel är överdriven säkerhetsklassning av personal. I verksamheter med höga säkerhetskrav kan många befattningar initialt placeras i säkerhetsklass, vilket är fullt motiverat utifrån den dåvarande hotbilden och verksamhetens inriktning. När roller, arbetsuppgifter eller verksamhetens förutsättningar senare förändras kan behovet av säkerhetsklassning i vissa delar av organisationen minska, medan det i andra delar kan kvarstå eller till och med öka.

Problemet uppstår när organisationen inte omprövar vilka befattningar som faktiskt behöver vara säkerhetsklassade i relation till den aktuella hotbilden. Om antalet säkerhetsprövade personer då förblir oförändrat trots att behovet minskat i delar av verksamheten, kvarstår kostnaderna för säkerhetsprövningsintervjuer, utbildningar och administrativ hantering utan motsvarande säkerhetsnytta. Resultatet blir ett personellt skydd som är överdimensionerat i förhållande till den faktiska risken och därmed kostnadsdrivande.

Överdrivna skyddsåtgärder uppstår även när skyddet inte tar hänsyn till mänskligt beteende. Ett vanligt exempel är mycket strikta och komplexa lösenordskrav. I syfte att höja säkerheten införs långa och svårhanterliga lösenord, vilket i praktiken leder till att medarbetare skriver ner dem på lappar, sparar dem oskyddat eller återanvänder dem på olämpliga sätt. Skyddsåtgärden blir dyr att administrera, genererar fler supportärenden och skapar nya sårbarheter, samtidigt som den faktiska säkerheten inte förbättras. I många fall hade enklare lösningar, kombinerade med tekniska begränsningar som spärrar efter upprepade felaktiga inloggningar, gett bättre skydd till lägre kostnad.

Ett liknande mönster kan ses i administrativt tungt säkerhetsarbete, där omfattande manuella kontroller, godkännanden och rutiner införs för att minimera risk. Dessa åtgärder kan ge en viss riskreduktion, men kräver stora mängder arbetstid och skapar friktion i verksamheten. Skadekostnaderna påverkas ofta marginellt, medan skyddskostnaderna ökar kraftigt.

Överdrivet skydd uppstår ofta när samma säkerhetskrav införs generellt i hela verksamheten, i stället för selektivt där de gör nytta. Alla system, lokaler eller processer omfattas av samma höga skyddsnivå, oavsett om de är verksamhetskritiska eller inte. Detta leder till höga skyddskostnader och ökad administrativ belastning, samtidigt som delar av skyddet inte bidrar till att minska relevanta risker.

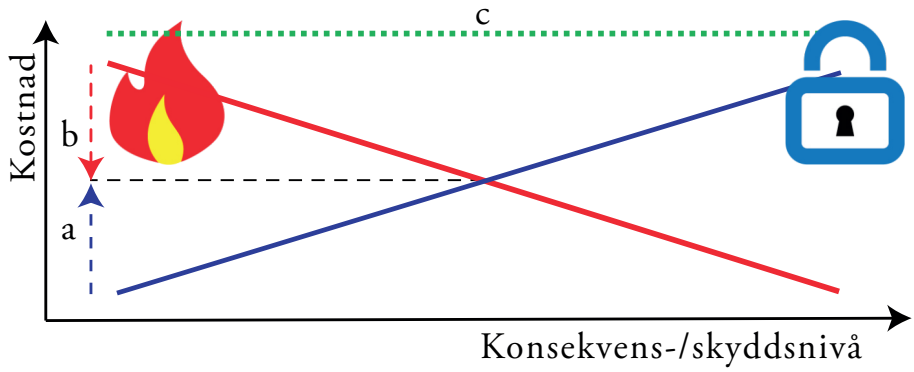
Redundans är i många fall en effektiv metod för verksamhetskritiska tillgångar, men kan bli överdriven när den införs utan tydlig analys. Ett exempel är när flera parallella system eller resurser införs, trots att verksamheten i praktiken saknar förmåga att använda dem vid en störning. Om organisationen inte har rutiner, utbildning eller bemanning för att faktiskt utnyttja redundansen blir den en kostsam försäkring utan verklig effekt på tillgänglighet eller skadekostnader.

Gemensamt för överdrivna skyddsåtgärder är att skyddet saknar proportionalitet i förhållande till tillgångarnas värde, hotbildens karaktär och konsekvensernas omfattning. Skyddsnivån drivs inte av aktuell riskanalys, utan av historik, rädsla, enskilda incidenter eller organisatorisk tröghet. Skyddet blir svårt att anpassa, dyrt att vidmakthålla och i vissa fall direkt hämmande för verksamheten.

Ur ett lönsamhetsperspektiv är överdrivna skyddsåtgärder det minst önskvärda tillståndet i modellen. Skyddet fungerar i någon mening, men utan att skapa ekonomiskt värde. Lönsam säkerhet kräver därför inte bara förmågan att förstärka skyddet när hotbilden ökar, utan också förmågan att justera, förenkla eller avveckla skydd när hotbilden minskar. Att våga växla ned skyddsnivån på ett kontrollerat och genomtänkt sätt är en central del av ett moget och lönsamt säkerhetsarbete.

Kompensatoriska skyddsåtgärder

Teoretiskt sett kan minskade skadekostnader och ökade skyddskostnader ta ut varandra, vilket innebär att skyddet inte blir lönsamt. Exempelvis om vi eftersträvar maximal säkerhet för att undgå alla skador. Vi utgår från att en högre skyddsnivå leder till en högre skyddskostnad (a). Ju högre skyddsnivå desto färre skador och lägre skadekostnader (b). Om skyddskostnaden ökar lika som skademinskningen förblir totalkostnaden (c) oförändrad, *break-even* och är inte lönsamt.



Kompensatoriska skyddsåtgärder är åtgärder som reducerar skadekostnader i ungefär samma omfattning som skyddskostnaderna ökar. Säkerheten förbättras, men den totala kostnaden för verksamheten förblir oförändrad, vilket innebär att åtgärderna inte leder till lönsamhet.

Ett vanligt exempel är överdimensionerad bemanning. Efter en incident väljer organisationen att öka antalet väktare eller säkerhetspersonal. Skadorna minskar, men personalkostnaderna ökar i motsvarande grad. Resultatet blir ett fungerande skydd, men utan ekonomisk nettoeffekt.

Ett annat exempel är tekniska skydd som överlappar varandra utan tydlig koppling till hotbilden. Flera larmsystem eller övervakningslösningar installeras för samma objekt, trots att hotbilden inte motiverar nivån av redundans. Skadekostnaderna minskar marginellt, medan investerings- och driftskostnaderna ökar lika mycket.

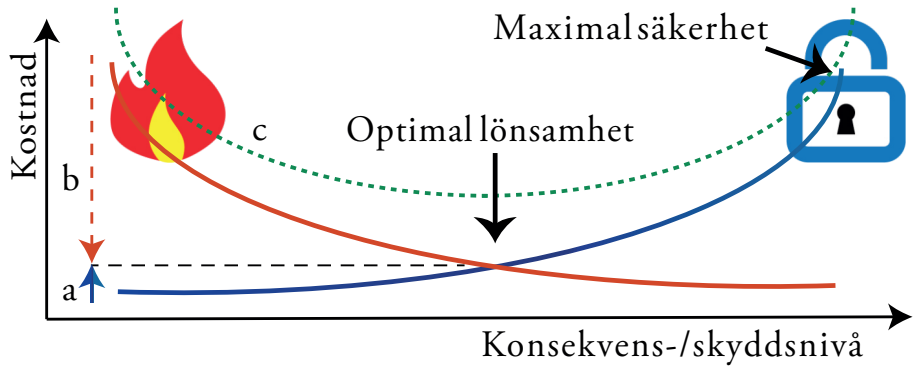
Även mycket hög skyddsnivå överallt i verksamheten är ett kompensatoriskt mönster. När alla områden ges samma skydd, oavsett om de är verksamhetskritiska eller inte, blir skyddskostnaderna höga samtidigt som en del av skyddet inte bidrar till att minska relevanta risker.

Slutligen förekommer kompensatoriska åtgärder i administrativt tungt säkerhetsarbete, där manuella kontroller och rutiner ersätter mer ändamålsenliga lösningar. Riskerna minskar, men arbetstiden och därmed kostnaderna ökar i samma takt.

Gemensamt för dessa exempel är att säkerhetsåtgärderna fungerar ur ett skyddsperspektiv, men skapar inte något ekonomiskt överskott. Skyddet kompenserar för skadorna, men totalkostnaden förblir oförändrad, ett klassiskt *break-even*-läge.

Optimala skyddsåtgärder

För att uppnå lönsamhet bör man sträva efter **optimal lönsamhet** snarare än **maximal säkerhet**. Optimal lönsamhet innebär att skador förebyggs i den utsträckning det är ekonomiskt motiverat. Det är sällan lönsamt att försöka förebygga alla tänkbara skador till varje pris. I vissa fall är det mer kostnadseffektivt att acceptera en kvarvarande risk och hantera konsekvensen när den inträffar.

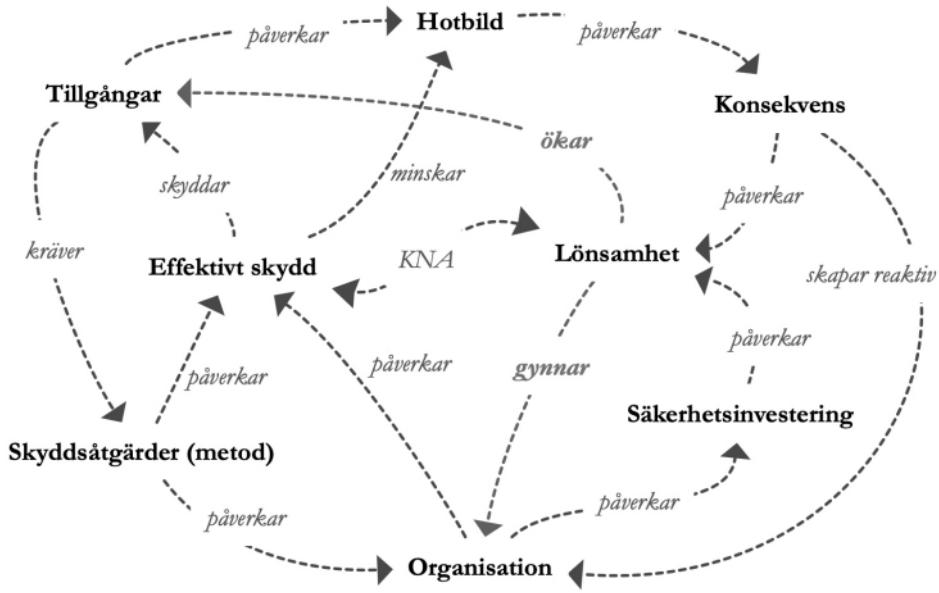


Optimal lönsamhet uppnås när skyddskostnaden (a) minskar skadekostnaden (b) mer än vad skyddskostnaden ökar, så att den totala kostnaden (c) blir så låg som möjligt. Fokus ligger inte på att minimera vare sig skyddskostnader eller skadekostnader var för sig, utan på att optimera helheten. För att uppnå detta behöver skyddskostnaderna optimeras genom att kombinera flera olika åtgärder på ett genomtänkt sätt, till exempel genom att:

- **prioritera kostnadseffektiva skyddsåtgärder,** där man börjar med billiga och effektiva åtgärder och är återhållsam med de dyraste och minst effektiva,
- tillämpa **skydd i flera lager** med kompletterande skyddsåtgärder,
- minimera risken för att en **enskild komponent** eller åtgärd blir en **kritisk svaghet** som äventyrar hela skyddet,
- skapa ett **balanserat skydd** med jämn skyddsnivå runt hela objektet,
- utforma skyddet **baserat på faktisk prestation** och skyddseffekt, snarare än enbart funktion eller teknisk lösning,
- införa **skyddsåtgärder i rätt ordning**, där upptäckt sker tidigt så nära perimetern som möjligt och följs av tillräcklig fördröjning fram till det skyddsvärda objektet, så att insats hinner fram för att avbryta och ingripa,
- säkerställa löpande **underhåll av skyddsåtgärderna** för att förhindra att skyddseffekten försämras över tid.

Sambanden mellan centrala områden

Det finns ett antal områden som påverkar förutsättningarna för lönsam säkerhet. Modellen för lönsam säkerhet bygger på åtta områden som tillsammans behöver beaktas för att säkerhetsarbetet ska bli effektivt, ekonomiskt och i slutänden lönsamt. Områdena är inte isolerade. De påverkar varandra i ett dynamiskt samband där förändringar i ett område leder till följdeffekter i flera andra. Att förstå dessa samband är avgörande för att kunna styra säkerhetsarbetet, inte bara beskriva det. Figuren nedan visar sambanden mellan områdena och hur de tillsammans driver skadekostnader, skyddskostnader och lönsamhet. Nedan följer en översikt av vad varje område innebär och hur det påverkar de andra.



Tillgångar – vad som ska skyddas och varför

Tillgångar handlar om att bestämma omfattningen av det som ska skyddas: **vad** tillgångarna är, **var** de finns, **vilka intressenter** som är involverade, **vilken betydelse** de har för verksamheten och vilka **krav** som ställs på skyddet.

De **skyddsvärda tillgångarna** kan delas in i **värdefulla tillgångar,** som har ett tydligt ekonomiskt värde och **verksamhetskritiska tillgångar**, som möjliggör eller genererar intäkter. En tillgång kan vara både värdefull och verksamhetskritisk. Tillgångarnas värde uttrycks i lämplig valuta och utgör grunden för den fortsatta analysen.

Tillgångarnas egenskaper, betydelse, sårbarhet och värde påverkar direkt hotbilden. Värdefulla eller verksamhetskritiska tillgångar tenderar att attrahera större, mer komplexa eller mer uthålliga hot, vilket ökar behovet av proportionerliga skyddsåtgärder.

Hotbild – nuläge och framtid

Hotbilden mot tillgångarna behöver identifieras för att kunna vidta proportionerliga skyddsåtgärder. Den kan bestå av både **naturliga** och **mänskliga** hot och omfatta både **direkt hotbild** och **överförd hotbild**, exempelvis via beroenden och omgivande system. Hotbilden behöver beskrivas i två tidsperspektiv. **Nuläge**, som ofta kan beskrivas med relativt hög säkerhet och **framtid**, som baseras på rimliga antaganden om utveckling över tid. Hotbilden kan exempelvis uttryckas som antal skador per år eller som procent av tillgångarnas värde per år.

Hotbilden påverkar konsekvenserna vid en säkerhetsincident. Ju större hotbild och ju större brist på skydd, desto allvarligare blir konsekvenserna när hot realiseras, vilket i sin tur påverkar verksamhetens ekonomi.

Konsekvens – direkta och indirekta skador

Konsekvens handlar om att undersöka hur stora **direkta** och **indirekta** skador som faktiskt har uppstått hittills på tillgångarna, givet de skyddsåtgärder som finns **idag**. Utifrån den förväntade **framtida** hotbilden bedöms även det förväntade skadeutfallet framåt i tiden. Konsekvens uttrycks som skadekostnader per år i lämplig valuta.

Konsekvenser av säkerhetsincidenter tenderar att driva fram ett reaktivt beteende, där åtgärder vidtas först efter att skadan redan inträffat. Detta leder ofta till ökade kostnader och sämre effektivitet jämfört med ett mer förebyggande arbetssätt. Stora konsekvenser leder till att skyddsåtgärdernas effektivitet behöver undersökas.

Metod – skydd och kontinuitet

Metod handlar om att välja **rätt typ av åtgärder** för rätt tillgångar och hotbild. Generellt gäller att **värdefulla tillgångar behöver skydd** mot skador och otillåten åtkomst. **Verksamhetskritiska tillgångar kräver kontinuitet**, exempelvis genom redundans. Metodvalet påverkar både skyddsnivå, skyddseffekt och hur organisationen behöver arbeta. Fel metodval kan leda till antingen onödigt höga skyddskostnader eller ökade skadekostnader.

Organisation – reaktivt och proaktivt säkerhetsarbete

Organisation omfattar alla som arbetar med eller påverkar säkerheten i verksamheten. Säkerhetsarbete kan bedrivas **reaktivt**, efter inträffade incidenter eller **proaktivt**, i förebyggande syfte.

Ett reaktivt arbetssätt är i regel mer kostnadsdrivande och mindre effektivt. Detta eftersom verksamheten drabbas av både en svårkontrollerad skadekostnad och en hastigt påkommen skyddsåtgärd med extra hög skyddskostnad. Ett proaktivt arbets-

sätt skapar bättre förutsättningar för hög skyddseffekt till en lägre skyddskostnad, lägre skadekostnader och mer förutsägbar ekonomi. Verksamhetens arbetssätt kan uttryckas som andelen mantimmar som läggs på proaktivt respektive reaktivt säkerhetsarbete.

Effektivitet – faktisk skyddseffekt

Effektivitet avser den faktiska **skyddseffekten** hos befintliga skyddsåtgärder i relation till hotbild och konsekvens. Utfallet behöver alltid tolkas i sitt sammanhang. Om inga konsekvenser har uppstått kan det bero på att skyddet är **tillräckligt**, men också på att skyddet är **överdimensionerat** och därmed hämmar verksamheten ekonomiskt. Om konsekvenser har uppstått kan det indikera att skyddet är **för svagt**, skyddar mot **fel hotbild** eller är **felaktigt implementerat**.

Effektivitet kan uttryckas i procent. Effektivitet uppstår i samspelet mellan valda skyddsåtgärder och organisationens arbetssätt. När effektiviteten är hög kan hotbilden även påverkas indirekt genom avskräckning eller genom att angrepp försvåras.

Investering – grund och löpande kostnader

Investeringar avser skyddskostnader och delas normalt upp i **grundinvesteringar**, som i huvudsak är engångskostnader, samt **löpande kostnader** som ackumuleras över året.

Investeringar uttrycks i lämplig valuta. Skyddsåtgärder och säkerhetsorganisation utgör investeringar som påverkar både effektivitet och lönsamhet. Investeringar med låg skyddseffekt ger begränsad nytta, medan investeringar med hög skyddseffekt kan reducera skadekostnader avsevärt.

Lönsamhet – kostnadseffekt och affärsnytta

Lönsamhet handlar om att analysera helheten av de säkerhetsrelaterade kostnaderna och intäkterna. Det omfattar **fördelningen mellan skyddskostnader och skadekostnader,** men även **möjliga intäkter** i form av nya affärsmöjligheter eller möjligheten att återfå annars förlorade tillgångar, exempelvis genom uppklarande av brott.

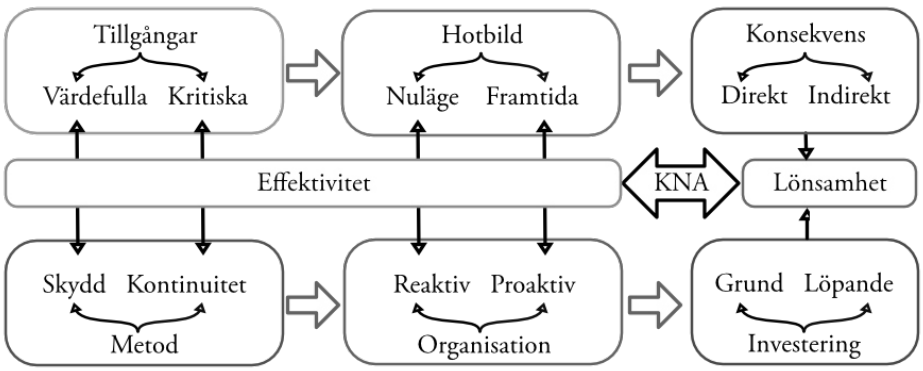
Kostnad–nytto-analys (KNA)

För att bedöma lönsamheten används ofta kostnad–nytto-analys (KNA) som ett verktyg för att väga skyddsåtgärdernas kostnad mot den förväntade nyttan i form av reducerade skadekostnader eller ökade intäkter. KNA fungerar därmed som en länk mellan effektivitet och lönsamhet.

I säkerhetssammanhang består nyttan ofta av minskad sannolikhet eller konsekvens för oönskade händelser, men kan även bestå av affärsnytta, exempelvis genom uppfyllda kundkrav, ökade affärsmöjligheter eller förbättrad leveransförmåga. KNA bidrar till att prioritera de åtgärder som ger störst effekt i förhållande till investerade resurser och till att fatta mer rationella och transparenta beslut.

Samtidigt är det viktigt att understryka att KNA inte ersätter analysen av tillgångar, hotbild och konsekvens. Analysen förutsätter att dessa är korrekt identifierade och värderade. En åtgärd med hög skyddseffekt är inte nödvändigtvis lönsam om kostnaden överstiger nyttan, medan en enklare åtgärd med måttlig effekt kan vara mycket lönsam om den kraftigt reducerar skadekostnader eller möjliggör affärer som annars inte varit möjliga.

KNA synliggör därmed sambanden mellan skyddskostnad och skadekostnad, mellan skyddseffekt och ekonomiskt utfall samt mellan kortsiktiga investeringar och långsiktig lönsamhet. I modellen för lönsam säkerhet blir analysen ett stöd för att se helheten och förstå hur olika beslut påverkar varandra över tid.



Figuren visar samband och påverkan mellan modellens delar. Pilarna beskriver riktning i besluts- och orsakssamband, inte beräkningar. Konsekvens, investering och lönsamhet är utfall av val och förutsättningar.

Modellen för lönsam säkerhet

Modellen för lönsam säkerhet beskriver hur säkerhetsarbete kan styras och prioriteras på ett sätt som både minskar risk och bidrar till verksamhetens lönsamhet. Utgångspunkten är att säkerhetsarbete aldrig är ett isolerat område, utan en integrerad del av verksamhetens värdeskapande.

I modellen utgår säkerhetsarbetet från **tillgångarna,** det som är värdefullt eller verksamhetskritiskt och som verksamheten är beroende av. Tillgångarnas egenskaper, värde och betydelse påverkar vilken **hotbild** de exponeras för, både i nuläget och över tid. Hotbilden avgör i sin tur vilka **konsekvenser** som kan uppstå om skyddet brister, i form av direkta och indirekta skadekostnader.

Hur **effektivt** dessa risker hanteras beror på valet av **metod**, till exempel skydd eller kontinuitet, samt på hur **organisationen** arbetar reaktivt eller proaktivt. Tillsammans påverkar dessa faktorer den faktiska **skyddseffekten**, det vill säga hur stor del av risken som reduceras i praktiken.

Säkerhetsarbete innebär alltid **investeringar**, både i form av grundinvesteringar och löpande kostnader. För att säkerhetsarbetet ska bli **lönsamt** behöver dessa investeringar stå i rimlig proportion till den nytta som uppnås, till exempel minskade skadekostnader, ökad stabilitet eller möjliggjorda affärer.

Här fungerar kostnad–nytto-analys (KNA) som ett viktigt beslutsstöd genom att synliggöra sambandet mellan skyddseffekt och ekonomiskt utfall.

Lönsam säkerhet uppstår när helheten optimeras, när rätt åtgärder vidtas, på rätt nivå och vid rätt tidpunkt, baserat på verksamhetens faktiska risker och mål. Modellen är därför cirkulär och dynamisk, inte linjär. Förändringar i verksamhet, hotbild eller omvärld kräver löpande omprövning av skyddsnivåer, arbetssätt och investeringar.

Modellen för lönsam säkerhet **kan tillämpas i både stort och smått**, från skyddet av ett helt land till skyddet av en enskild tillgång. I praktiken kan modellen behöva tolkas och anpassas efter verksamhetens förutsättningar, men principerna är desamma oavsett omfattning.

Modellens åtta delar kan användas som ett övergripande **stöd för minnet** eller brytas ned till **detaljerade analyser och beräkningar** när så behövs. Båda angreppssätten leder till ett mer medvetet och lönsamt säkerhetsarbete.

I de följande kapitlen fördjupas modellens olika delar, med start i tillgångarna – grunden för allt säkerhetsarbete och den första byggstenen i lönsam säkerhet.

Tillämpning

För större verksamheter kan det vara ändamålsenligt att börja i liten skala. Ett sätt är att samla nyckelpersoner från olika delar av verksamheten och genomföra arbetet med hjälp av **arbetsboken**, som en workshop avgränsad till en mindre del av verksamheten. På så sätt ges möjlighet att lära sig arbetssättet och genomföra hela modellen under en begränsad tidsperiod.

Därefter kan deltagarna ta med sig det gemensamma arbetssättet tillbaka till sina respektive verksamhetsdelar och fortsätta arbetet lokalt. Detta är ofta ett resurseffektivt sätt att både höja säkerhetsmedvetandet och skapa förutsättningar för ett mer lönsamt säkerhetsarbete.