Säkerhet i en ny tid

En presentation av CANEA och SRS


Hur kan vi skapa ett sammanhängande och systematiskt säkerhetsarbete som möter en förändrad hotbild och ökade krav från kunder, lagstiftning och omvärld?

Agenda

1. Bakgrund och förändrade krav
2. Säkerhetsstrategi
3. Grundpelare för systematiskt säkerhetsarbete
4. Säkerhetskultur
5. ISO 27001 som stöd för säkerhetsstrategin
6. Nästa steg

Bakgrund

Ökad hotbild och hårdare krav

Ny och förändrad hotbild

Rapport: Kärnkraftsföretag hackades

2017-07-07 09:00 Av: TT

Rysslands invasion av Ukraina

”Anlitas för ett uppdrag – sen är de förbrukade”

Näringsliv Börs Tech

OMX-S -0,32% DOW -1,07% € 10,99 $ 9,45 ,58% Sivers Semiconductors: 55,70

Gängens pengar

313 svenska politiker kopplas till gängen

Våg av kidnappni

Stor hackerhärva till Ryssland avsl

UPPDATERAD 17 APRIL 2026 PUBLICERAD 16 APR

Data visar att hackare med kopplinga
stort antal e-postkonton tillhörande högt uppsatta tjänstem
Ukraina, samt i flera Natoländer och ryska allierade. Det visa
granskning gjord av Reuters.

Dagens AI-drivna cyberattacker är geopolitiskt motiverade och mer hänsynslösa än någonsin förr

Cyberattacker riktas mot allt från elnät till valsystem. AI används som ett vapen som aldrig tar paus.

Polisens larm: Infiltreras av gängkriminella

Publicerad 6 okt 2023 kl 13.43
Uppdaterad kl 18.23

Det läcker information från polisr gängen.
Det menar poliskommissarien D
– Hur stor skada det gör beror p

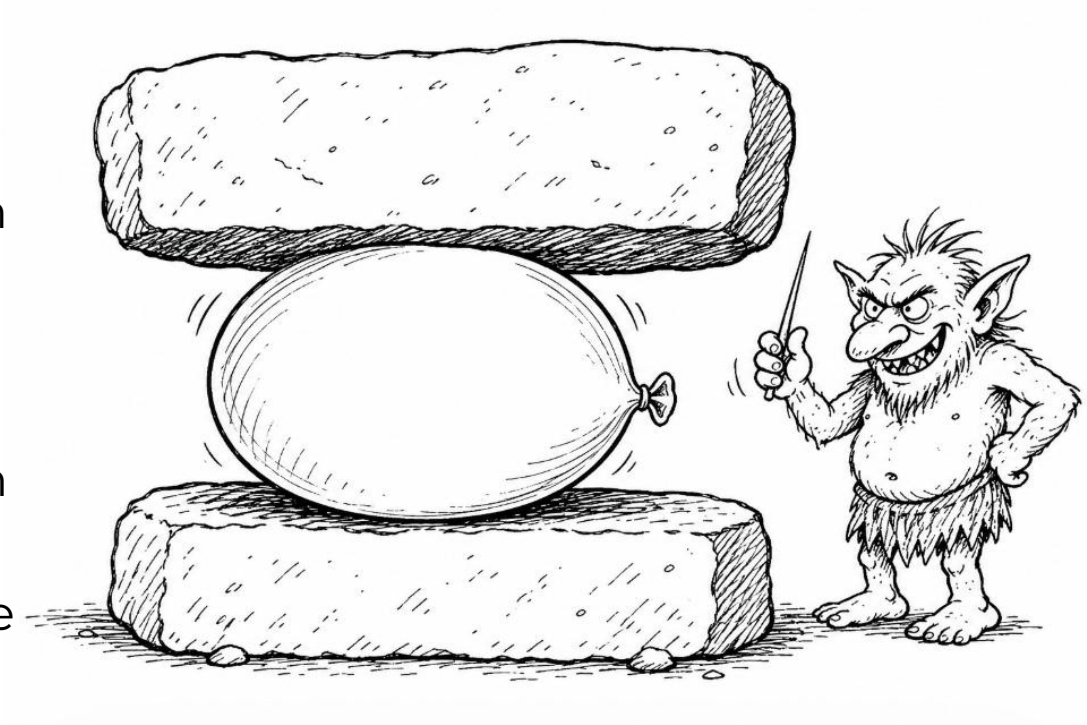
Nationalmuseum hackat – skickar ut phishingmejl

UPPDATERAD 6 MAJ 2026 PUBLICERAD 5 MAJ 2026

E-postmeddelanden, så kallade phishingmejl, skickas från en av Nationalmuseums officiella e-postadresser med en länk till ett dokument. Museet bekräftar att en medarbetares e-post har hackats.

Säkerhet i en ny tid

- Hoten ökar i omfattning och komplexitet.
- Konsekvenserna av incidenter kan vara ödesdigra
- Utökat och skärpt regelverk med bl.a. NIS2, CER, …
- Ökade kundkrav – säkerhet blir en del av kvalitetsbegreppet
- Ökade krav från ägare och styrelse – Kritiska risker måste hanteras



Vanliga utmaningar kring säkerhetsarbetet

- Säkerhet ses som ett IT-problem istället för ett ledningsansvar
- Dålig kunskap om hot, sårbarheter och risker
- Överfokus på verktyg istället för processer
- Svag koppling mellan säkerhet och affärsmål
- Bristande engagemang och kompetens hos ledningen
- Personberoende
- Resurserna har inte ökat i takt med kraven, snarare tvärt om

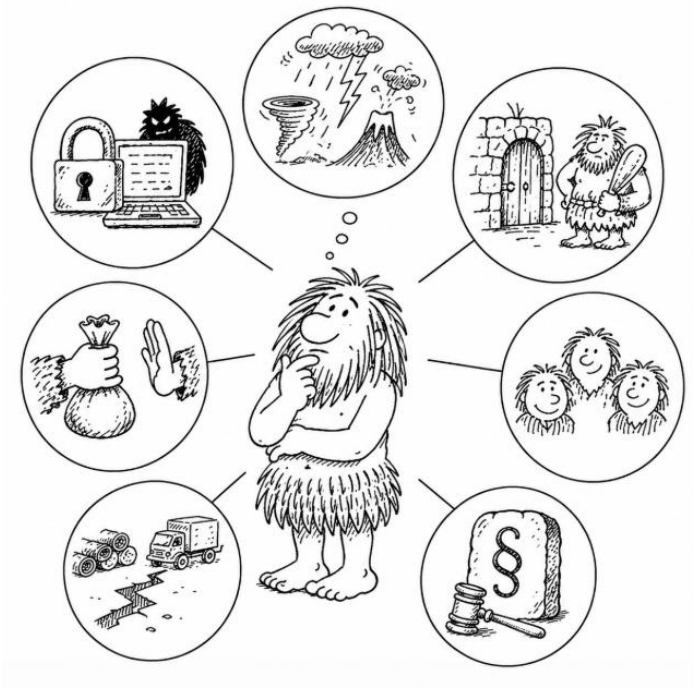
Säkerhetsstrategi

Ett helhetsgrepp kring organisationens säkerhet

Säkerhetsstrategi

För att möta kraven och utmaningarna behöver organisationen ta fram en tydlig säkerhetsstrategi utifrån ett helhetsperspektiv:

- Fysisk säkerhet
- Naturkatastrofer
- Informationssäkerhet
- Cybersäkerhet
- IT och nätverkssäkerhet
- Personalrelaterad säkerhet
- Säkerhet i leverantörsleden



Frågor att besvara i strategin

VAD är skyddsvärt?	• Vad är kritiskt och skyddsvärt i organisationen? • Vilka krav och förväntningar har våra intressenter?
Vad är hotbilden?	• Vilken kontext befinner sig organisationen i? • Hur ser hotbilden ut mot vår verksamhet? • Vilka sårbarheter finns det i verksamheten?
Hur hanterar vi hotbilden?	• Vilka är säkerhetsriskerna? • Hur ska riskerna prioriteras och hanteras? • Hur ska vi organisera oss för att få bästa effekt? • Hur ska vi möta förändringar? • Hur ska vi utvärdera och förbättra våra processer?

Grundpelare för systematiskt säkerhetsarbete

Förståelse för kontext och hotbild

Varför?

- Rätt skydd kräver rätt hotbild- åtgärder behöver dimensioneras utifrån de verkliga hot som verksamheten står inför
- Koppling till affärs- och verksamhetsrisker
- Proaktivt istället för reaktivt säkerhetsarbete

Exempel på metoder

- Omvärldsanalys och trendspaning
- Intern analys
- Threat Modeling - Kartlägga potentiella angripare
- Informationsdelning och underrättelser (t.ex., CERT-SE, ENISA)
- Interna erfarenheter och information från incidenter, revisioner och avvikelser

Kunskap om sårbarheter

Varför?

- Sårbarheter krävs för hot att ska kunna realiseras
- Kunskap om sårbarheter gör proaktiva åtgärder möjliga
- Kunskap om sårbarheter ger underlag för prioriteringar och resursallokering

Exempel på metoder

- Tekniska sårbarhetsskanningar (cybersäkerhet)
- Fysisk säkerhetsgranskning (”björnligan”)
- Simulerade attacker som phishing, tailgating eller social engineering
- Revision, intervjuer och workshops
- Tidigare incidenter och avvikelser

Riskbaserad analys och prioritering

Varför?

- Resurser är begränsade - styr säkerhetsarbetet mot det som är mest kritiskt
- Underlag för strategiska beslut - möjlighet att balansera skyddsnivåer, kostnader och acceptans utifrån verksamhetsmål
- Riskperspektivet är ofta även ett absolut krav i både standarder och lagstiftning

Exempel på metoder

- Klassisk riskanalys
- Tillgångsbaserad riskanalys
- Scenariobaserad analys
- Riskregister och verktyg för riskuppföljning
- Workshops och tvärfunktionella riskdialoger

Dokumentation

Varför?

- Skapar tydlig struktur, spårbarhet och ansvar
- Möjliggör intern styrning och extern granskning
- Underlättar lärande och kontinuerlig förbättring
- Krav på dokumentation i många regelverk

Exempel på metoder

- Policyer, processer, riktlinjer, rutiner
- Dokumentation av riskanalyser och åtgärdsplaner
- Händelseloggar, incidentrapporter
- Lärandematerial
- Tillgänglig och rollanpassad dokumentation
- Dokumenthanteringssystem (t.ex. CANEA ONE)

Förebyggande arbete

Varför?

- Minskar risken att hot realiseras
- Skapar motståndskraft och trygghet i verksamheten
- Lägre kostnader än reaktiv hantering

Exempel på metoder

- Tekniska kontroller och säkerhetskonfigurationer
- Fysisk säkerhet och åtkomstskydd
- Bakgrundskontroller,
- Säkerhetsmedvetenhet och utbildning
- Process- och systemdesign
- Granskningar, revisioner och kontroller

Incident och krishantering

Varför?

- Alla organisationer kommer förr eller senare at råka ut för incidenter
- Avgörande för att minimera skador och återställa verksamheten
- Krav från kunder, myndigheter och standarder

Exempel på metoder

- Kontinuitetsplaner och krisplaner
- Incidenthanteringsprocess
- Roller, ansvar och kontaktlistor
- Övningar och simulerade händelser
- Efteranalys och lärande efter incident

Systematik och ständig förbättring

Varför?

- Säkerhet är en levande process – inte ett projekt
- Systematik ger långsiktighet, spårbarhet och ansvar - inte beroende av eldsjälar eller ad hoc-lösningar
- Förbättring bygger på mätning, lärande och ledningens engagemang

Exempel på metoder

- PDCA (generell metodik för förbättringsarbete)
- Ledningssystem för informationssäkerhet (ISMS)
- Interna och externa revisioner och granskningar
- Uppföljning av mål och mätetal
- Avvikelsehantering
- Test av planer och beredskap
- Sårbarhetsanalyser

Säkerhetskultur

Säkerhetskultur

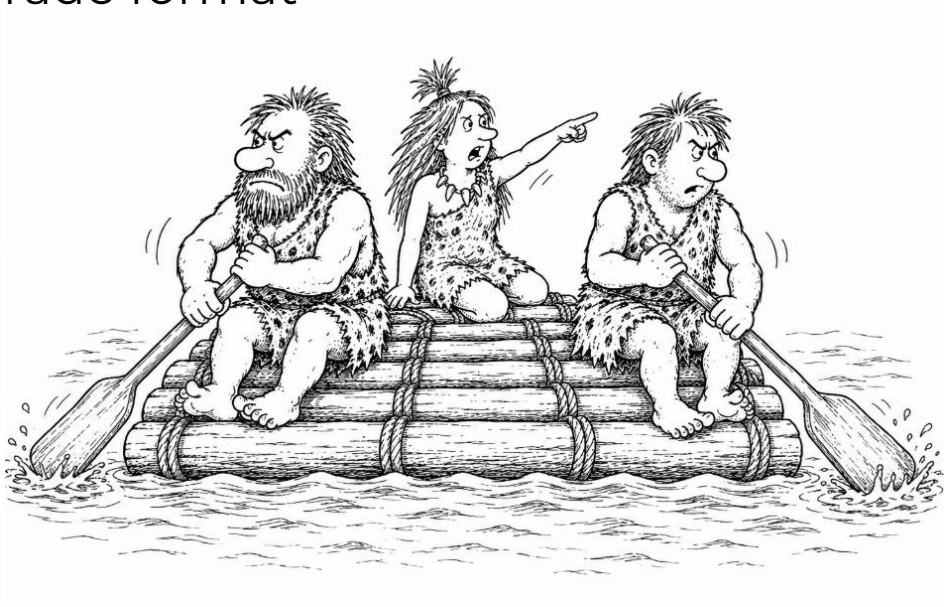
Utan en stark säkerhetskultur blir säkerhetsarbete en administrativ pålaga – med rätt kultur blir det en naturlig del av verksamheten.

- Ett effektivt säkerhetsarbete bygger inte enbart på processer, policyer och kontroller, utan i hög grad på organisationens kultur.
- Kulturen styr beteenden i vardagen
- Kultur minskar behovet av detaljstyrning
- Ledningens ansvar att etablera och befästa denna kultur

Varför blir säkerhetsarbete ofta ineffektivt?

Säkerhetsarbete blir ineffektivt och ansträngande när det byggs parallellt med andra ledningsstrukturer och processer i verksamheten.

- Arbetet drar åt olika håll utifrån olika intressen
- Dubbelarbete och onödigt komplicerade format
- Dokumentation utan användning
- Personberoende arbetssätt
- Svag koppling till affären



ISO 27001 som grund för det systematiska säkerhetsarbetet

ISO´s standarder för ledningssystem

ISO ´s standarder ger beprövade modeller för att leda och styra verksamheten på ett systematiskt sätt utifrån krav och behov inom olika områden. De bygger på metoder och ”best practice” som ledande experter inom området enats om.

NIS2 kräver systematik – ISO 27001 levererar strukturen

- Förståelse för organisationens kontext och förutsättningar
- Ledningens engagemang
- Riskbaserad analys och prioritering
- Försvar med flera lager av åtgärder
- Revision, mätning och ständig förbättring
- Systematisk utvärdering av resultaten
- EU (ENISA) och myndigheter refererar till ISO 27001/27002


SVENSK STANDARD
SS-ISO/IEC 27001:2022

Informationssäkerhet- Cybersäkerhet och integritetsskydd – Ledningssystem för informationssäkerhet – Krav (ISO/IEC 27001:2022, IDT)

Information technology – Cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022, IDT)

SIS Svenska Institutet för Standarder

Language: svenska/Swedish, engelska/English

Utgåva: 3, Edition: 3

SIS enanvändarlicens/SIS single user license: CANEA Partner Group AB, beställd av/ordered by: Nicolas ter Wissche, Ordernummer/ordernumber: 2053265264, beställningsdatum/order date: 2023-01-23

Från krav till konkurrenskraft

Bonus!

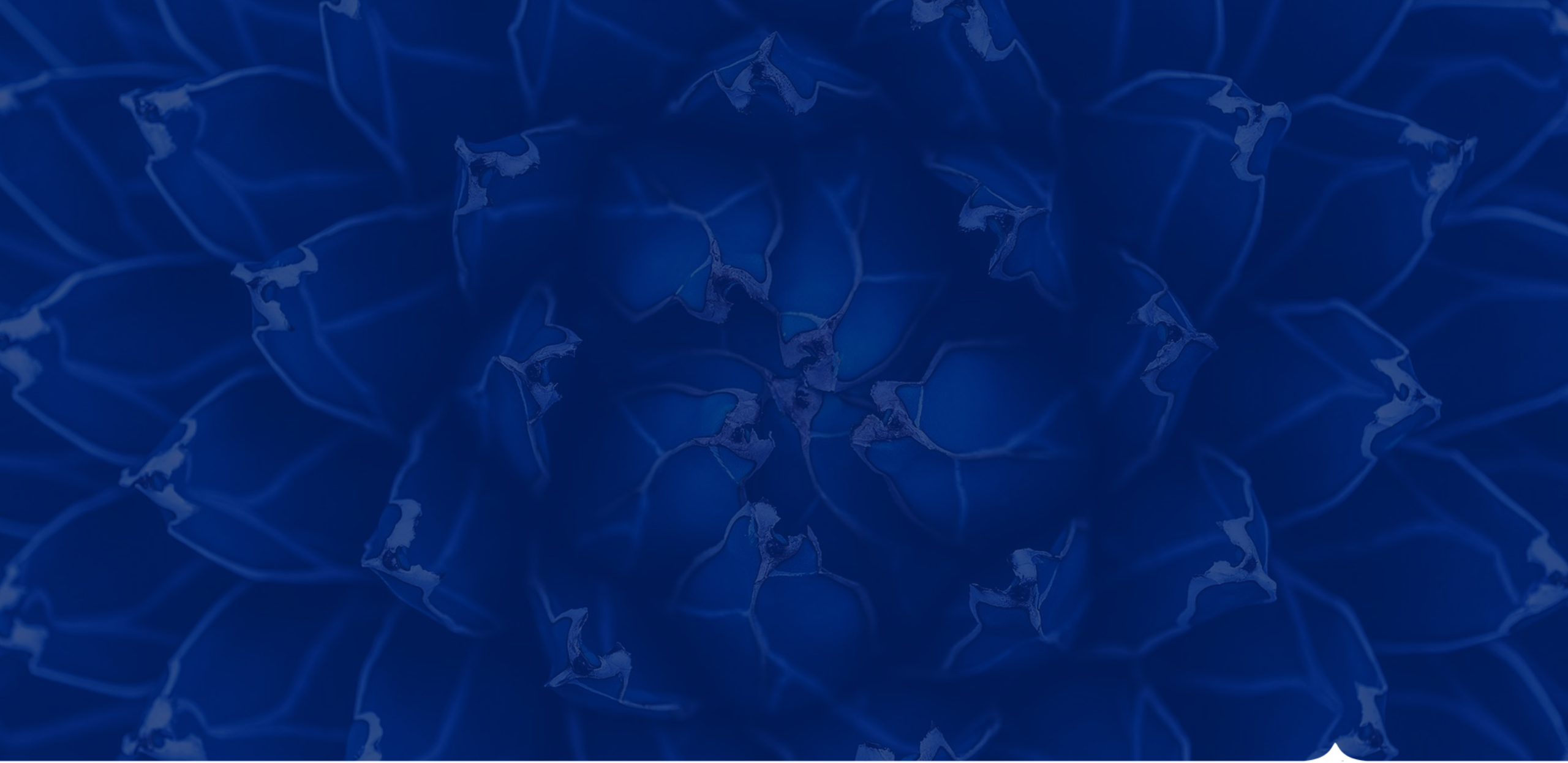
Rätt utformat bidrar ett systematiskt säkerhetsarbete inte enbart till krav- och regelefterlevnad utan även till operativ effektivitet och affärsnytta.

- Minskad dubbelarbete
- Ökad operativ effektivitet
- Starkare kundförtroende
- Systematiskt förbättringsarbete
- Bättre beslutsunderlag
- Fungerande arbetssätt är skalbara

Nästa steg

Nästa steg

- GAP-analys mot relevanta krav (t.ex. NIS2/MCFs föreskrifter)
- Ledningsworkshop/ Utbildning för ledningen
- Beslut och handlingsplan framåt
- Implementeringsprojekt
- (Certifiering)



CANEA