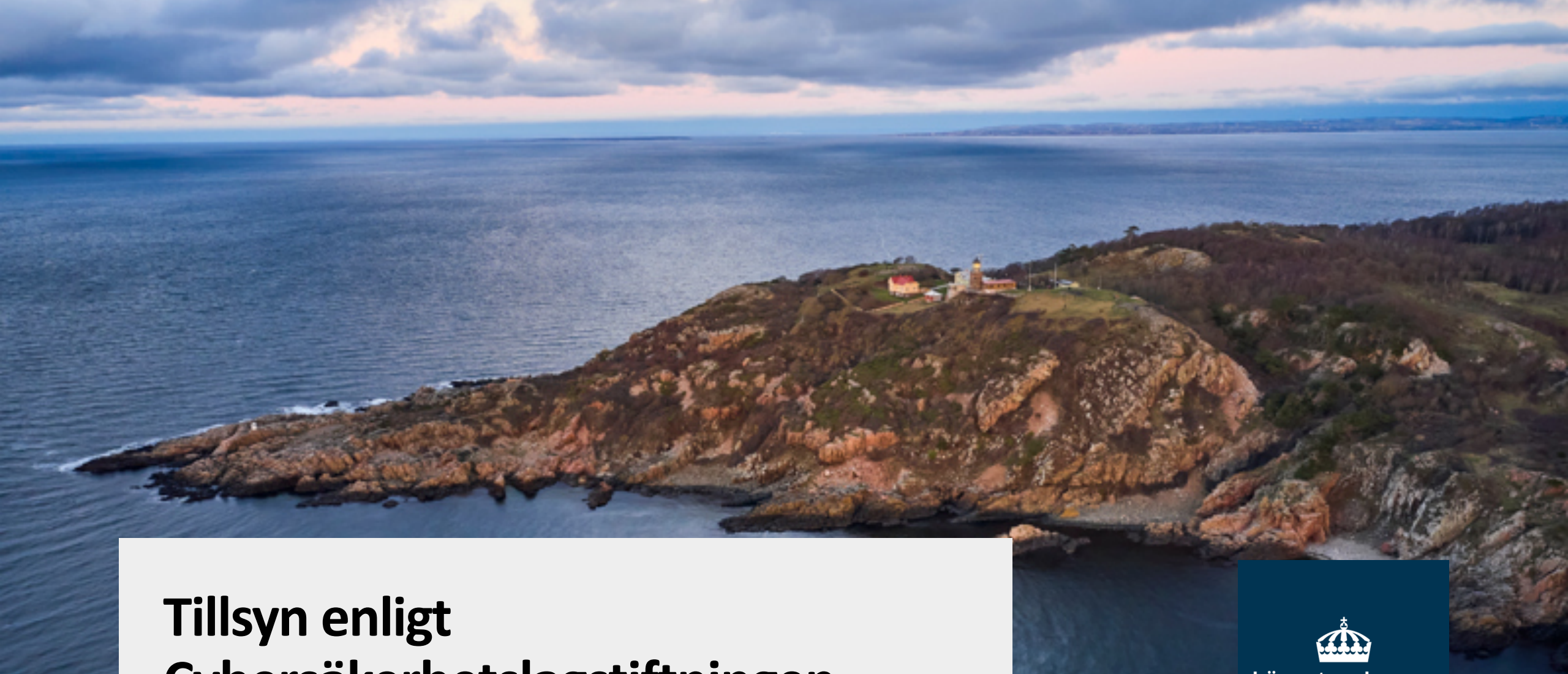


Tillsyn enligt Cybersäkerhetslagstiftningen

Marie Louise Arendt

Chef för tillsyn säkerhetsskydd, cybersäkerhet, Länsstyrelsen Skåne

Länsstyrelserna

Agenda - en överflygning

1. Varför finns Cybersäkerhetslagen?
2. Väsentliga och viktiga verksamhets-utövare
3. Tillsynsmyndigheter och deras roll
4. Olika typer av tillsyn
5. Vad tittar tillsynen på?
6. Hur går tillsyn till?
7. Vad vill tillsynsmyndigheten se?
8. Vanliga brister
9. Hur kan man förbereda sig?

1. Varför finns lagen?

NIS2 är en uppföljning av EUs första NIS-direktiv från 2016

De främsta skälen för NIS2 är:

- Digitaliseringens framsteg
- Ransomware, DDoS-attacker och dataintrång har ökat i omfattning och sofistikering
- Geopolitiska hot, cyberattacker används som verktyg i konflikter

2. *Väsentliga* och *viktiga* verksamhetsutövare

I EU finns det regler som specificerar vad som är **mikro**, **små**, **medelstora** och **stora** företag.

Huvudregel för att omfattas av Cybersäkerhetslagen är att verksamhetsutövaren är ett **medelstort företag eller större**

Vid beräkning av storlek tas hänsyn till ***antingen*** antalet anställda, omsättning ***eller*** balansomslutning

Huvudregeln är att det är **årsarbetskrafter** som ska beräknas och de finansiella uppgifterna hämtas från företagets egna räkenskaper

CSL: Medelstort företag eller större

Beräkningsgrund	Medelstort företag	Stora företag
Antal årsarbetskrafter	50-249 årsarbetskrafter	250 + årsarbetskrafter
Årsomsättning	Upp till 50 miljoner euro	Mer än 50 miljoner euro
Balansomslutning	Upp till 43 miljoner euro	Mer än 43 miljoner euro
	Viktiga	Väsentliga

Länsstyrelserna

13 stycken tillsynsmyndigheter (vara 6 st Länsstyrelser)

3. Tillsynsmyndigheter

Energimyndigheten	Energi
Finansinspektionen	Bankverksamhet, Finansmarknadsinfrastruktur
Livsmedelsverket	Avloppsvatten, Dricksvatten, Produktion, bearbetning och distribution av livsmedel
Läkemedelsverket	Hälso- och sjukvårdssektorn, Tillverkning av medicintekniska produkter och medicintekniska produkter för in vitrodiagnostik
Länsstyrelserna	Avfallshantering, Forskning, Lärosäten med examenstillstånd, Offentlig förvaltning, Tillverkning, produktion och distribution av kemikalier m.fl.
Inspektionen för vård och omsorg	Vårdgivare i hälso- och sjukvårdssektorn
Post- och telestyrelsen	Digital infrastruktur, Digitala leverantörer m.fl.
Transportstyrelsen	Transporter, tillverkning (motorfordon släpfordon, påhängsvagnar och andra transportmedel)

Länsstyrelserna

3. … och deras roll

VÅRT SYFTE: ÖKA CYBERSÄKERHETEN OCH BYGGA ETT STARKT, MOTSTÅNDSKRAFTIGT SAMHÄLLE

Tillsynsmyndighetens roll är att säkerställa att organisationer följer lagstiftningen och upprätthåller en hög nivå av cybersäkerhet och motståndskraft mot incidenter

- Inte för tillsynsmyndighetens skull
- Inte för den enskilda organisationens skull
- Utan för Sveriges och samhällets skull

Länsstyrelserna

TYPER AV TILLSYN

Fem sätt att välja ut organisationer eller områden för tillsyn

1. PLANERAD TILLSYN

Man bestämmer i förväg att vissa organisationer ska bli föremål för tillsyn, t.ex. för att det var länge sedan sist.

TILLSYNS-PLAN →

Organisationer i turordning

EXEMPEL

Alla organisationer inom en sektor får tillsyn regelbundet enligt plan.

VERKSAMHETSUTÖVARE

Väsentliga verksamhetsutövare

5. Vad tittar tillsynen på?

- Dokumentation och uppföljning
- Incidenthantering
- Kontinuitet och återställningsförmåga
- Ledningsstyrning och ansvar
- Leverantörsstyrning och leverantörskedjor
- Riskanalyser och riskhantering
- Tekniska säkerhetsåtgärder
- Utbildning och säkerhetskultur
- Verifiering och tester

5. Hur tittar vi?

Vi tittar på dokument, men inte bara!

Vi intervjuar, och granskar på plats:

- Hur styrning fungerar
- Att ansvar är tydliga
- Att systematiska åtgärder finns
- Om dessa genomförs
- Om riskhantering leder till beslut
- Och om det finns ett lärande

Tillsynsmyndighetens roll i cybersäkerhetsekosystemet

Vi skapar förutsättningar för ett säkrare och mer motståndskraftigt samhälle

7. Vad vill tillsynsmyn-digheten se?

Vi vill normalt se:

- Ansvar
- Vilja
- Styrning
- Utveckling och förbättringsförmåga
- Riskmedvetenhet

En mogen verksamhet med identifierade bris-ter bedöms ofta annorlunda än en omogen verksamhet utan engagemang och kontroll

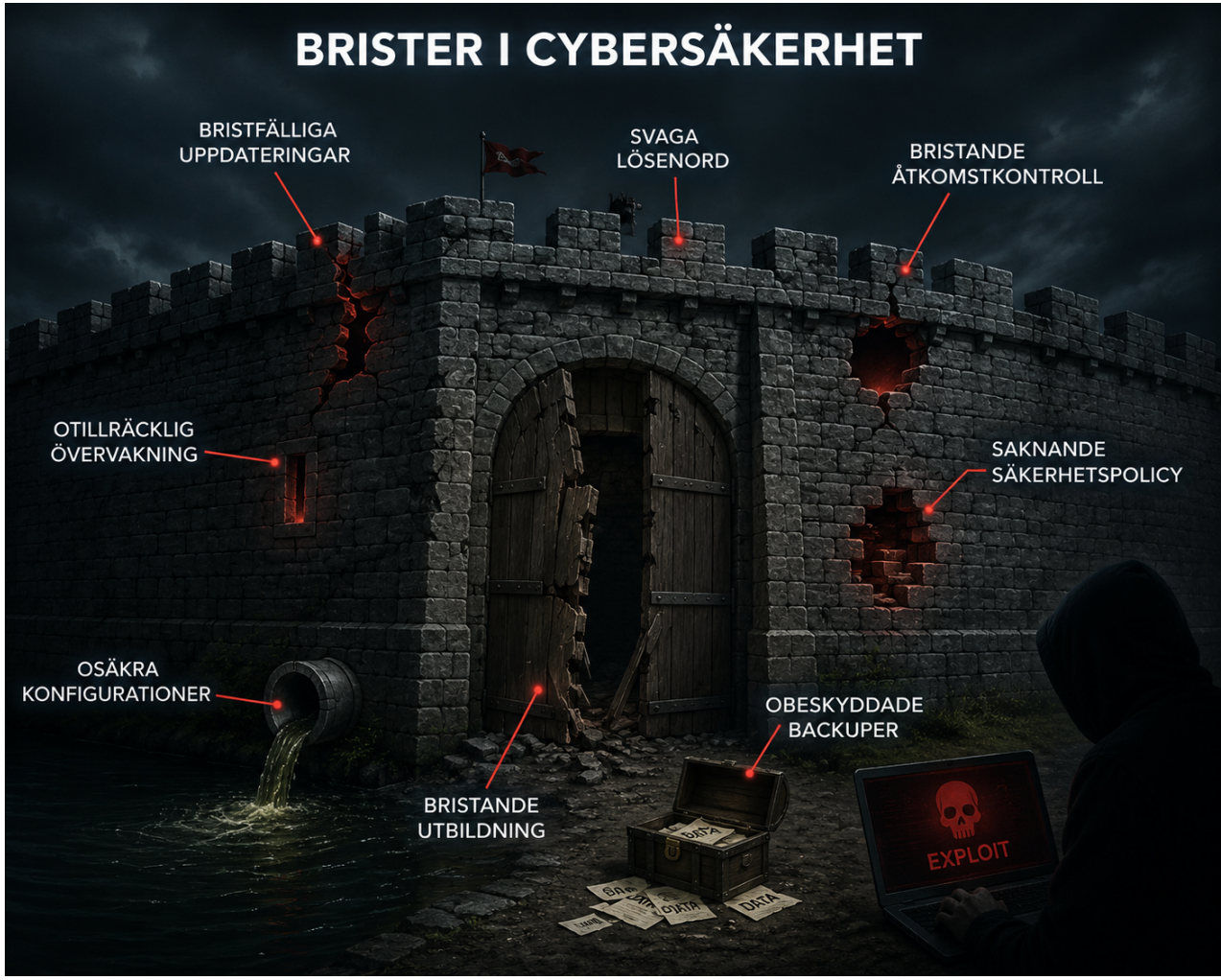
8. Vanliga bri er

…är som regel antingen *organisa-toriska*, *processuella* eller *tek-niska*

- Otydligt ansvar
- Otillräcklig ledningsförank-ring
- Låg kunskap om cyber-säkerhet
- Svag leverantörsstyrning
- Bristande riskmetodik
- Rutiner finns men följs inte

8. Vanliga brister

- Man gör sårbarhetsscanningar men åtgärdar inte sårbarheterna
- Ser pentester som en engångsföreteelse
- Genomför ingen faktisk uppföljning
- För stort fokus på policy istället för förmåga
- Bristande kontinuitetsarbete
- Otydliga incidentprocesser: när, hur, vem?
- Otillräckliga tekniska åtgärder



Länsstyrelserna

9. Hur *kan* man förbereda sig?

Börja med att förstå om och varför er verksamhet omfattas

Gör en verksamhets- och omfattningsanalys där ni identifierar:

- vilka delar av verksamheten som omfattas,
- vilka tjänster som är kritiska,
- vilka system och processer som stödjer dem,
- vilka beroenden som finns,och
- vilken kategori verksamheten tillhör: ***väsentlig***, eller ***viktig***

9. Hur *kan* man förbereda sig?

Identifiera skyddsvärden och kritiska beroenden. Det gör ni t ex genom:

- Informationsklassning
- Systemkartläggning
- Processkartläggning
- Beroendeanalys
- Leverantörsanalys

9. Hur *kan* man förbereda sig?

Sen är det bra att göra riskanalyser, för helheten och per system:

- Hot
- Sårbarheter
- Sannolikhet
- Konsekvenser
- Eliminerande/mitigerande åtgärder
- Prioritering och proportionalitet
- Riskacceptans

9. Hur *kan* man förbereda sig?

I nästa steg tar ni fram säkerhetsåtgärder:

Tekniska:

- Brandväggar, segmentering, kryptering, backup, loggning, patchhantering, SOC/SIEM etc

Processuella:

- Incidenthantering, change management, accesshante-ring, backup- och återställningsprocesser, kontinuitets-processer, sårbarhetsscanning, pentester och leveran-törshantering, logg- och övervakningsprocesser …

Organisatoriska:

- Styrning, ansvar, roller, beslutsvägar, utbildning/kompe-tens, kultur

Länsstyrelserna

9. Hur *kan* man förbereda sig?

Därefter:

Uppföljning och förbättring!

Allt hänger ihop:
People, Process, Technology

Många organisationer är **tekniskt starka**, men *processuellt svaga*:

- larm finns, men:
- ingen vet vem som ska agera,
- det finns inga eskaleringsvägar,
- incidenter dokumenteras inte,
- lessons learned genomförs inte.

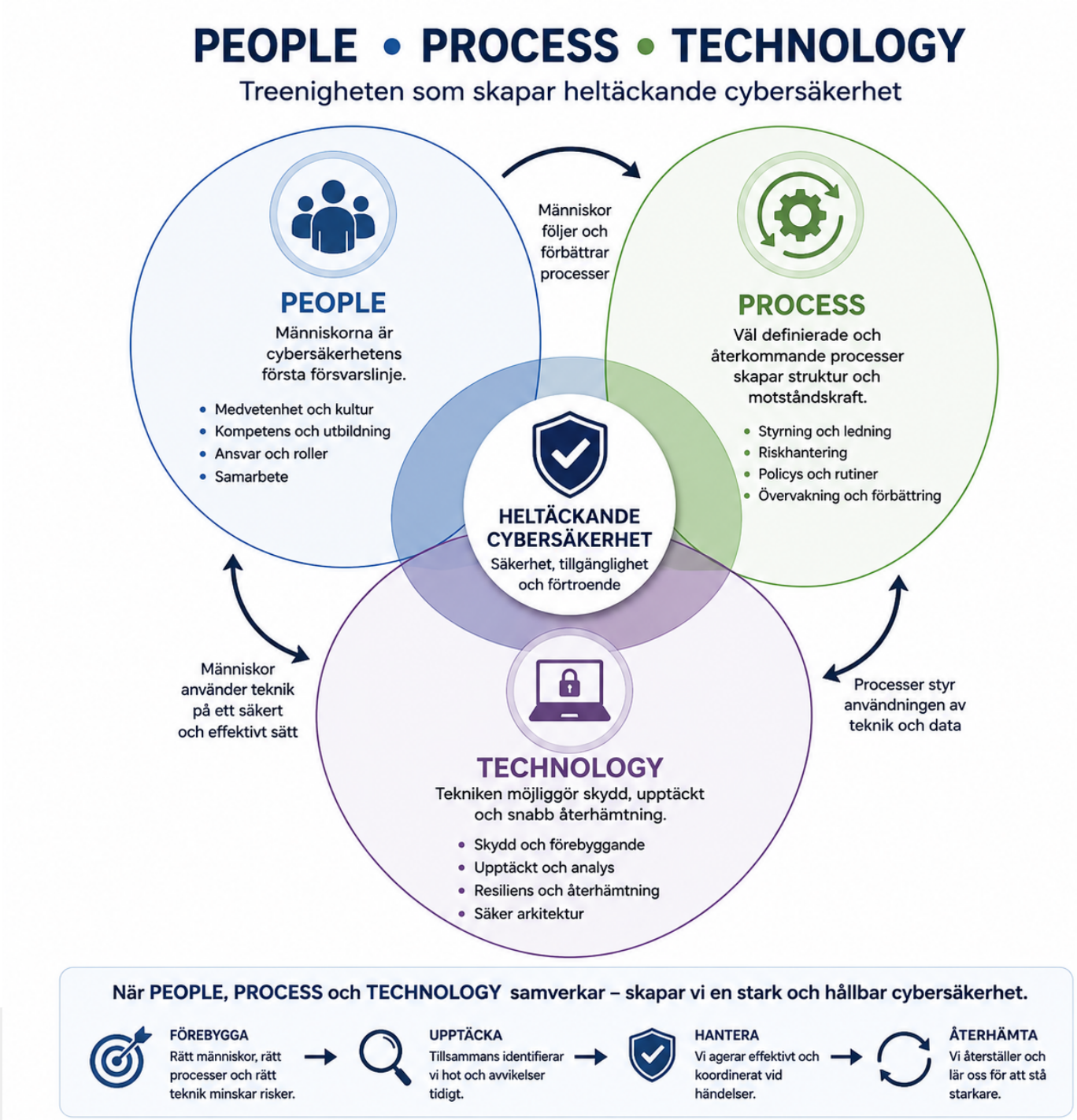
Då hjälper tekniken inte särskilt mycket.

Andra organisationer har **bra processbeskrivningar**:

- men *inte tillräckliga tekniska förmågor*
- eller *okunniga medarbetare* som utsätter organisationen för risk

Då fungerar det inte heller!

People, Process, Technology



Men vägledning, då?

- I tillsynsmyndighetens uppdrag finns ord som ”tillsyn” och ”efterlevnad”
- Inte ”rådgivning”, ”vägledning” eller ”stöd”
- Men, vi ger det ändå
- Vi vill att ni ska skydda er del av Sverige
- Det vore dumt att inte hjälpa er med det om vi kan
- Så, meddela oss vad ni vill veta mer om
- Vi har redan genomfört 3 webinar och vi kommer göra fler
- Berätta vad ni behöver!

Läs mer på MCFs hemsida! Sök på *”Det här är cybersäkerhetslagen”*

Och, glöm inte att anmäla er!

Om verksamheten bedömer att de omfattas av cybersäkerhetslagen ska verksamhetsutövaren anmäla sig till Myndigheten för Civilt Försvar (MCF).

- *Anmälan görs genom att kontakta nis2anmalan@mcf.se för vidare instruktioner om hur anmälan under reservförfarandet går till*
- *En anmälan ska göras så snart det kan ske*

Det går att förbereda sig inför anmälan genom att ta del av formuläret som finns på myndighetens webbplats (MCF).

I formuläret finns det också hjälptexter som förklarar vilken typ av information som ska lämnas

Det här är cybersäkerhetslagen

Länsstyrelserna

Frågor?

skane@lansstyrelsen.se

Länsstyrelserna