

Nationella Säkerhetsdagen

Säkerhetsarbete på en större myndighet

Lars Hjelm

Lars Hjelm

Chef Cybersäkerhet, Försäkringskassan

IT-säkerhetschef



- **Bor** - Sundsvall
- **Ålder** - 50+
- **Familj** - Gift, två vuxna döttrar
- **Fritidsintressen** - Fjäll & friluftsliv, fiske, foto, motorcyklar, teknik, m.m.

Försäkringskassan

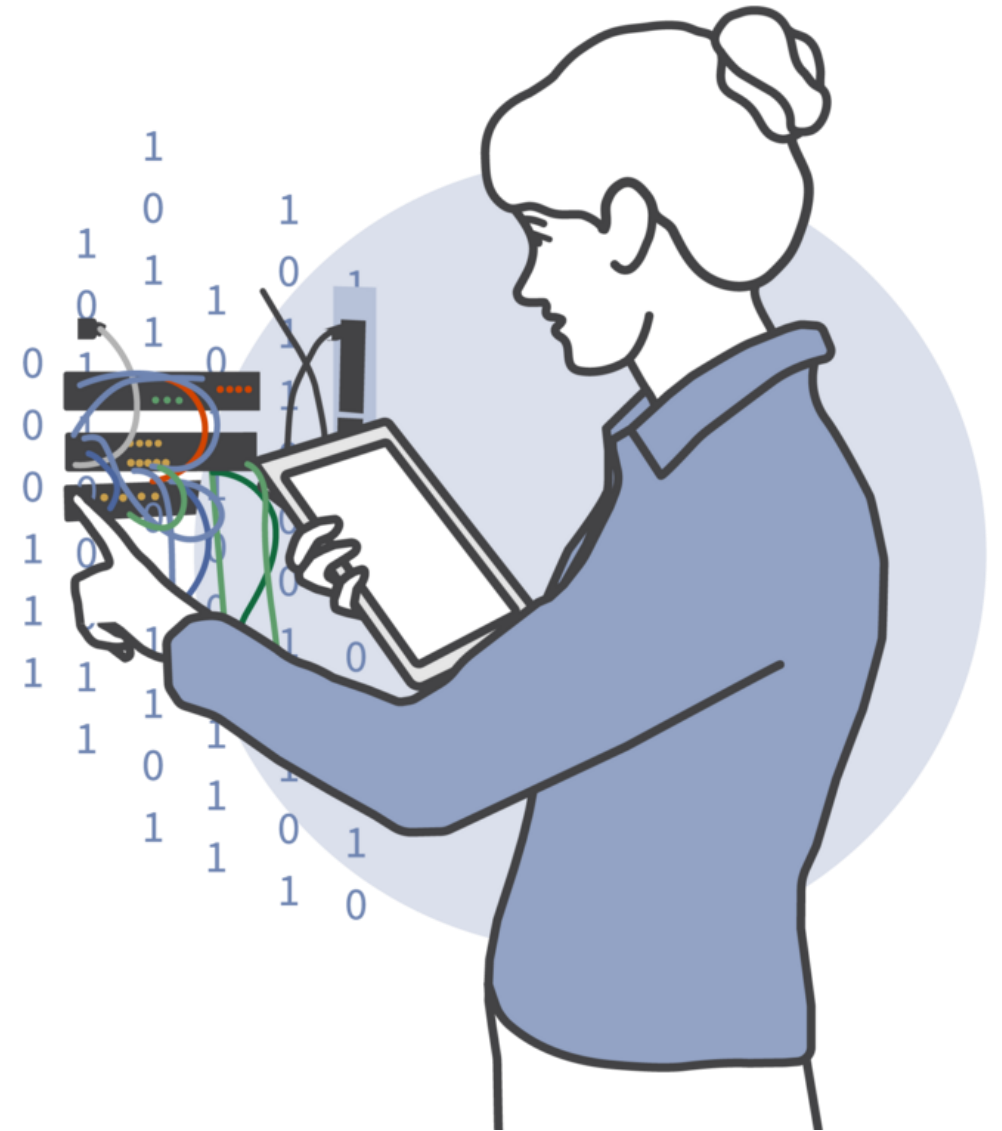
Försäkringskassans digitalisering

- 68 miljoner besök per år på forsakringskassan.se
 - 39 miljoner besök på Mina Sidor
 - 11,6 miljoner digitala ansökningar per år
 - 83% av alla ansökningar sker digitalt
 - 99% ansöker om Föräldrapenning digitalt
 - Sedan 2013 har vi ersatt över 52 miljoner pappersutskick med digitala meddelanden ...
- ... men vi skickar fortfarande ut 18,6 miljoner pappersförsändelser varje år

IT-avdelningens uppdrag

- Utveckla, drifva och underhålla Försäkringskassans alla IT-tjänster.
- Utveckla och förvalta myndighetens tvärfunktionella lösningar för digital samverkan, både internt och externt.
- Utveckling eller drift av IT-tjänster för Pensionsmyndigheten, Myndigheten för digital förvaltning, Statens Servicecenter och många fler.

Vår vision är att vara Sveriges bästa IT-avdelning, hur man än mäter.

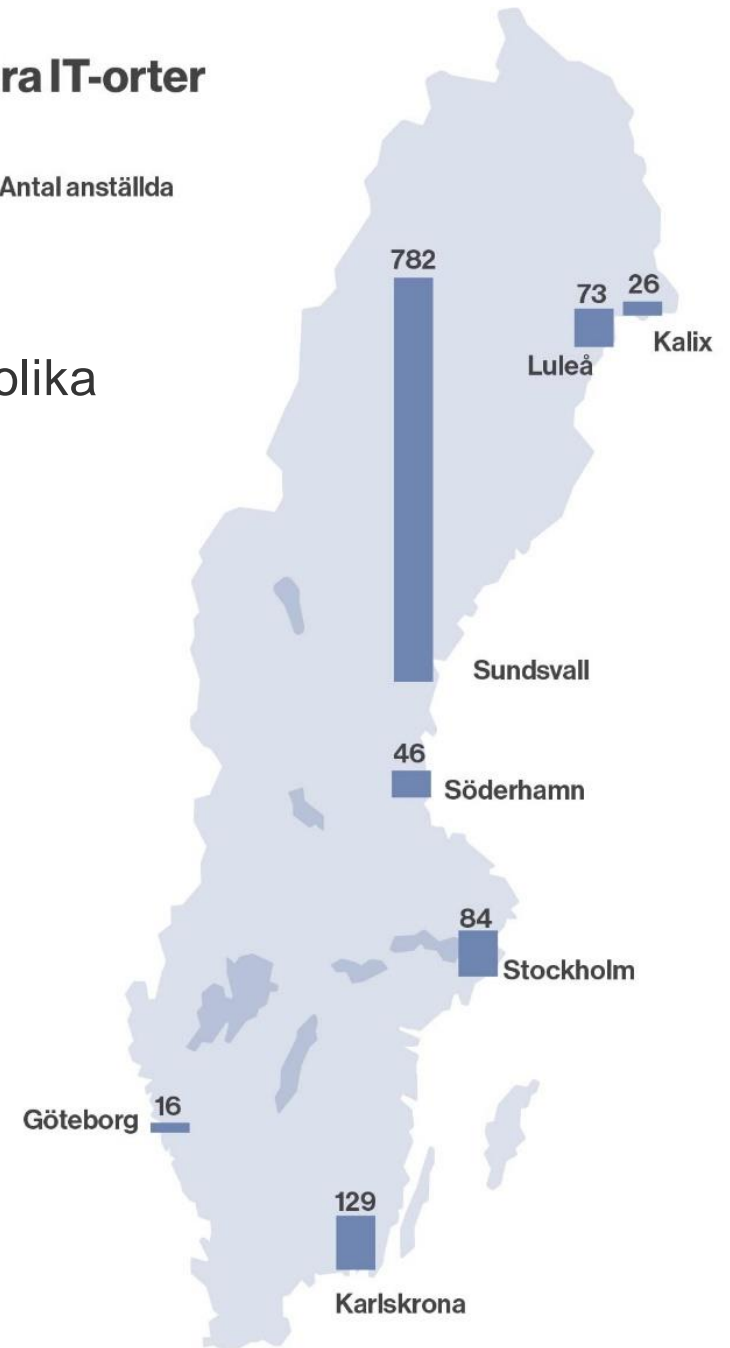


IT - Snabba fakta

- Utveckling för ca 700 miljoner kr i 100 parallella projekt årligen.
- Vi hanterar 54 it-tjänster. Dessa består i sin tur av mer än 200 olika delsystem och produkter.
- Drift av mer än 13 000 servrar, 6 000 terabyte data och 20 000 it-arbetsplatser.
- IT-tjänsterna hanterar årligen:
 - 485 miljarder kr i utbetalningar
 - 39 miljoner besökare på mina sidor
 - 99 miljoner samtal och digitala interaktioner
- Avdelningen omsätter 2,1 miljarder kronor och har mer än 1200 anställda verksamma på 7 orter.
- IT-direktör Peter Haglind.

Våra IT-orter

■ Antal anställda



Ett av Sveriges största datacenter

485 000 000 000

kronor betalades ut via våra system under 2019

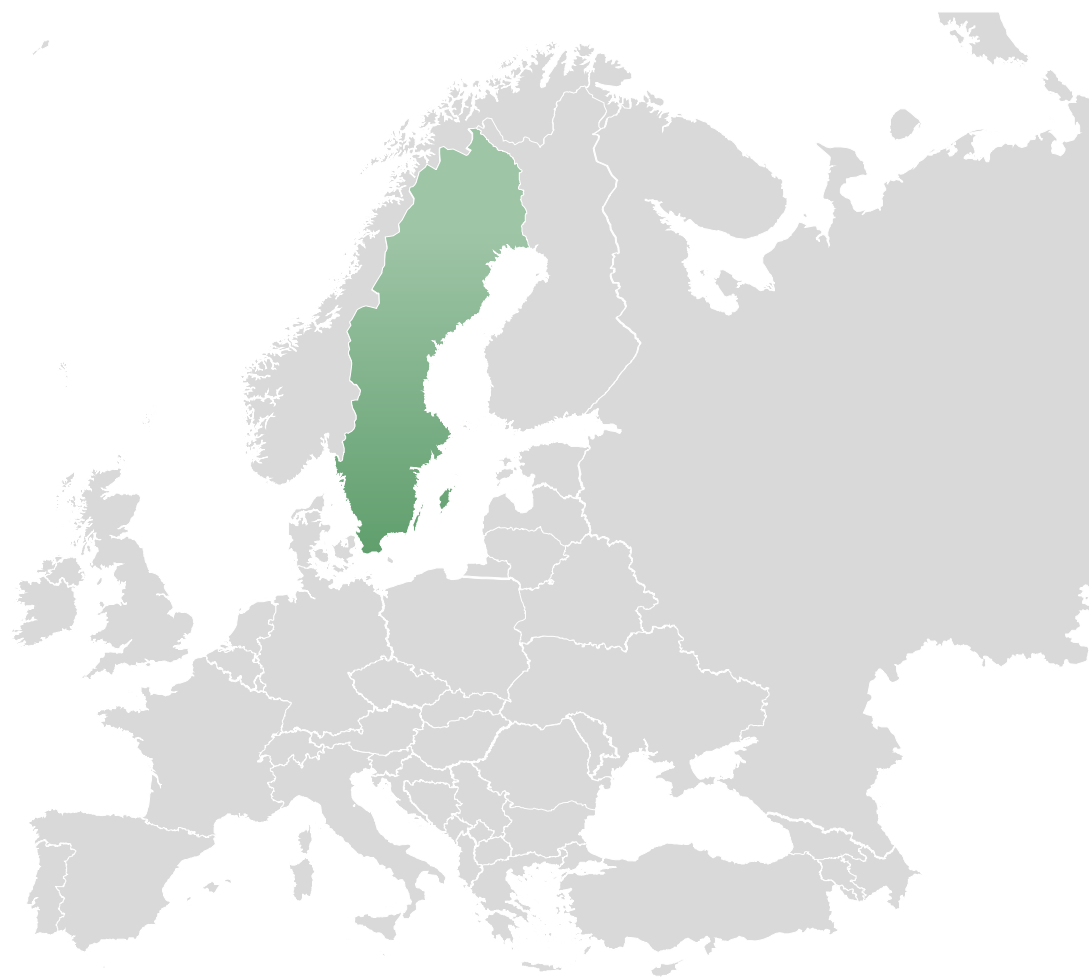


13 000
SERVAR

6 000 terabyte
lagrad information

Samordnad och säker statlig it-drift

- Regeringen ger Försäkringskassan i uppdrag att 2017-2022 erbjuda en samordnad och säker it-drift för vissa myndigheter
- Det övergripande syftet är att utvärdera former för samordnad och säker it-drift för lämpliga myndigheter



1 Säkerhet

2 Effektivitet

3 Digitalisering

4 Små myndigheter

FK IT-produktion i korthet

54 IT-tjänster, 200 delsystem

utveckling – drift – underhåll

9 kundmyndigheter

har tecknat samverkansöverenskommelse

465
medarbetare



FK IT-utveckling i siffror



100

PARALLELLA PROJEKT

900 000

UTVECKLINGSTIMMAR



640

ANSTÄLLDA

650 M
UTVECKLING

150 M
UNDERHÅLL



Säkerhetskänslig verksamhet

- Försäkringskassan bedriver säkerhetskänslig verksamhet och omfattas därmed av säkerhetsskyddslagstiftningen.
- *”Säkerhetsskydd handlar om att skydda den information och de verksamheter som är av betydelse för Sveriges säkerhet mot spioneri, sabotage, terroristbrott och vissa andra hot.”*



Grundläggande säkerhetsarbete

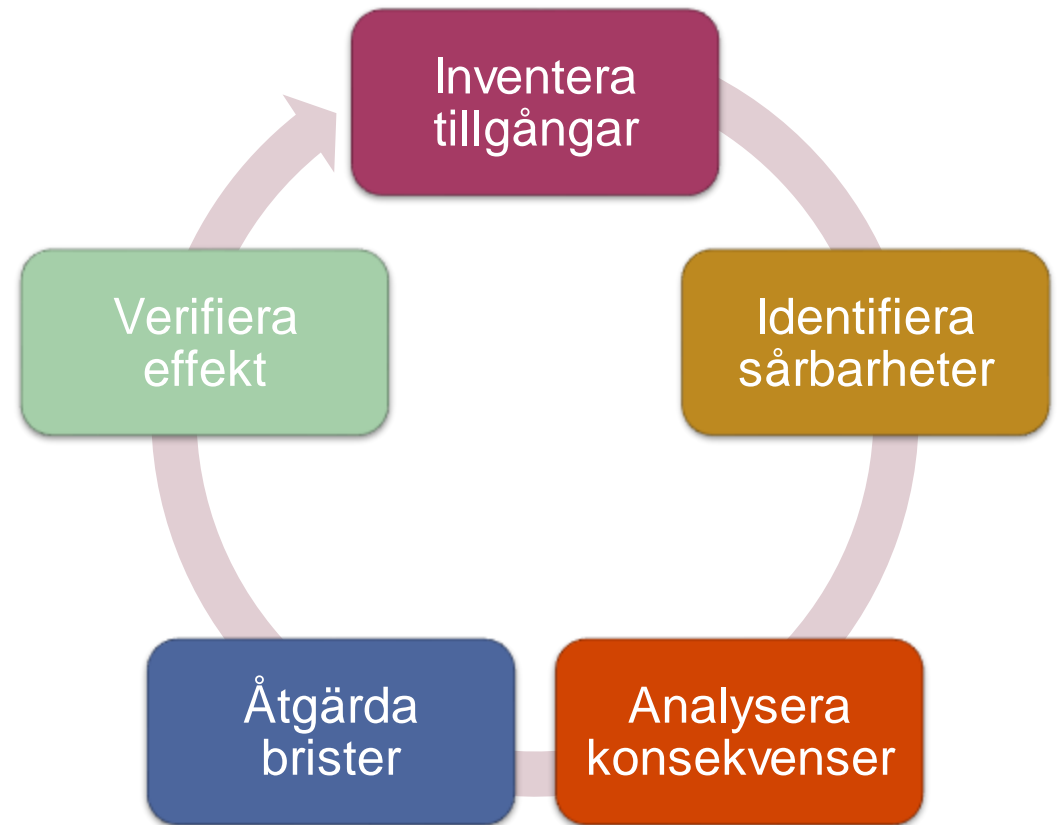
- ✓ Systematiskt säkerhetsarbete
- ✓ Aktuell hotbild & lämpliga skyddsåtgärder
- ✓ Begripliga säkerhetsregler
- ✓ Datasäkring & återläsningstester
- ✓ Säkra identiteter & multifaktor autentisering
- ✓ Spårbarhet & loggning
- ✓ Rollseparering
- ✓ SOC-funktion
- ✓ Säkerhetsgranskningar
- ✓ Efterlevnadskontroller
- ✓ Utbilda & bygg en god säkerhetskultur
- ✓ Skydda mailen
- ✓ Penetrationstester
- ✓ Kontinuitetsövningar



Security Operation Center - SOC

Några nyckelfaktorer:

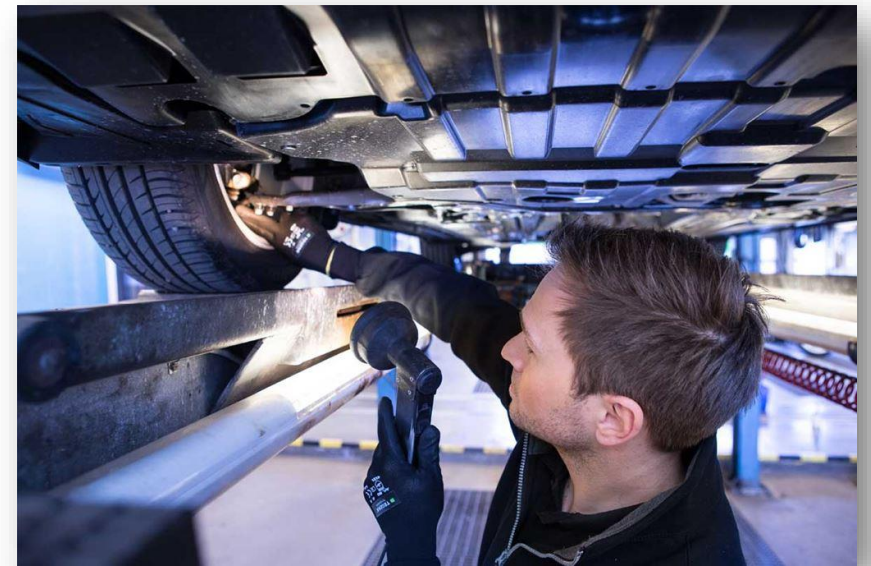
- Säkerställ data för analys
 - Loggar, larm, hotbild, omvärldsbevakning, samverkan
- Robust tillgångshantering
 - Vad ska skyddas?
 - Vem ska åtgärda?
- Automatiserade sårbarhetsskanningar
 - Kontinuerliga skanningar
- Etablerad process för att åtgärda brister
 - Ärendehantering
 - Rätt prioriteringar
 - Snabb hantering
- Rapportera säkerhetsläget regelbundet



Säkerhets CCB (Change Control Board)

- Granskar tekniska ändringar som kan påverka säkerheten

- Bemannas med erfarna säkerhetsresurser
 - Erfarenheter från SOC-funktionen
 - Likande ärenden, återkommande trafikflöden
- Underlag för granskning
 - Beskrivning av ärendet
 - Systemskiss/lösningensbeskrivning
 - Tekniska förutsättningar
- Risker & Konsekvenser
 - Riskanalys
- Beslutsprocess
 - Riskacceptans
 - Säkerhetsmedvetna beslut
 - Dispenshantering



Säkra system – hela vägen!



Aktuella utmaningar

- Förändrad hotbild
 - NATO medlemskap
 - Geopolitiska läget
 - Perimeterskydd räcker inte längre
- Supply chain
 - Viss desperation finns efter hårdvara, har vi tillräcklig kontroll på försörjningskedjorna?
- Felsökningar i verksamhetskritiska system på distans?
 - Supportärenden kräver ofta data från vår infrastruktur – hur/vad delar vi?
 - Digital ledsagning?
- Ökat distansarbete
 - Attraktiv arbetsgivare
 - Svårt att hitta kompetens
 - Fokus på funktioner för distansarbete



Gör vi rätt saker – är vi säkra nu?



- Köper, bygger & utvecklar vi säkra IT-lösningar?
- Övervakar vi rätt saker - har vi örat mot rätt räl?
- Har alla förstått säkerhetsreglerna?
- Hur vet vi att reglerna efterlevs?
- Har vi ett riskbaserat arbetssätt – tar vi säkerhetsmedvetna beslut?
- Märker vi alla attackförsök?
- Har vi tillräcklig förmåga att agera snabbt?

Samverkan!



- Vi behöver kanaler att dela aktuell information
- Informationsdelning måste ske snabbt och enkelt
- Vi måste kunna lita på riktigheten i delad information
- Erfarenhetsutbyte inom Sverige

”Samverkan kan ses som ett organisatoriskt sätt att lösa utmanande uppgifter som den egna enheten inte klarar på egen hand. Samverkan kan också beskrivas som en form av systematiserande samarbete. För att samverkan ska fungera behövs styrning, struktur och samsyn”

NIST **FRA** **Upphandling** **PEN tester** **DDoS**
ISO 27001/2 **Säpo** **Lagstöd** **Ledningssystem för Informationssäkerhet (LIS)**
Ethical hacking **GDPR** **Normering** **Dispensansökan**
Flerkundsdrift **Hotbild** **Säkerhetsprövning**
Molntjänster **Säkerhetskultur** **Säkerhetsskyddslagen** **SIEM**
Revisioner **Informationsklassificering** **Arkitektur**
Tekniska skyddsåtgärder

