Informations- & cybersäkerhet i vindkraften

Digitaliserade och fysiska hot

Per Olofsson
Roger Klahr

2021-11-01

Agenda

- Mål och syfte med denna presentation
  - Att ge en översiktlig bild om hot och risker inom el- branschen
  - Peka på konkreta utmaningar
  - Visa på möjligheter
- Händelser i vår ”omvärld”
- NIS- direktivet
- Säkerhetsskyddslagstiftningen
- Systematiskt informationssäkerhetsarbete (ISO 27000)
- Konkreta tips

Kort presentation

Per Olofsson

- 20 års erfarenhet från IT branschen med 14 år i Energibranschen
- Teknikintresse sedan 286:ans tid
- W3 Energy - Den största oberoende förvaltaren av vindkraft

Roger Klahr

- 30 års erfarenhet av fysisk säkerhet samt verksamhetsstyrning inom IT
- Utbildare inom informationssäkerhet
- Erfarenhet från kommuner och regionen
- Väl förtrogen med lagstiftningen inom säkerhetsområdet

1990 - Internet (som vi känner det) *"föds"*

- Under 1990-talet började privatpersoner använda nätet i större utsträckning, då kommersiella operatörer erbjöd förbindelser åt hemanvändare och World Wide Web slog igenom.
- På 1990-talet uppstod World Wide Web (WWW), med internet som grund. Den första webbläsaren skapades av Tim Berners-Lee på Cern 1990.
- I samma tider började internetförbindelser erbjudas också kommersiellt. Windows 95 stödde internet och därmed blev det lätt för PC-användare i hemmen att koppla upp sig.
- Dessa nya användare blev i första hand erbjudna sin internetleverantörs webbportal och förblev ofta omedvetna om många av de andra tjänsterna på internet.

Internet of Things (IoT)

- **Sakernas internet** (från engelskans *Internet of Things*, *IoT*)
- Ett samlingsnamn för de tekniker som gör att vardagsföremål som hushållsapparater, kläder och accessoarer, men även maskiner, fordon och byggnader, med inbyggd elektronik och internetuppkoppling, kan styras eller utbyta data över nätet.

Drönarrobot som både flyger och går

Drönarroboten Leonardo kan flyga, gå, åka skateboard och gå på lina. Mångsidigheten ska göra det enklare för Leonardo att orientera sig i skiftande terräng.

– Leonardo kan röra sig genom utmanande miljöer mer effektivt än traditionella robotar genom att växla mellan sina tillgängliga rörelsemedel, säger Kyunam Kim, forskare på Caltech, som utvecklat drönarroboten.

Namnet Leonardo är en förkortning för legs onboard drone. Genom sina fyra propellrar kan den 75 centimeter höga och 2,58 kilo tunga roboten, utöver att gå, även balansera på lina och åka skateboard. När det väl är dags att ta sig upp för trappor kan Leonardo flyga.

Leonardo, även kallad Leo, kan överbrygga gapet som just nu finns mellan robotar och drönare.

På grund av dess förmåga att hantera sluttande och ojämna terränger finns det, enligt Caltech, även scenarion där drönarroboten kan göra nytta på Mars.

Källa: The Verge, Feber

27 OKTOBER 2021REPORTER FREDRIK ADOLFSSONDIGITFOTO CALTECH

Energi- och oljebolag betalar oftast vid ransomware

Allt eftersom ransomwareattacker ökar blir det tydligare vilka branscher som är mest villiga att betala lösensummor. Industriföretag är minst betalningsvilliga medan energi- och oljebolag betalar ut mest frekvent, visar en ny studie.

Mindre än var femte företag inom tillverkande industri, närmare bestämt 19 procent, uppger att de betalat lösensummor efter att ha utsatts för en ransomwareattack. Det globala genomsnittet ligger på 32 procent. Mest betalningsvilliga är energi- och oljebolag där 43 procent uppger att betalat angriparna.

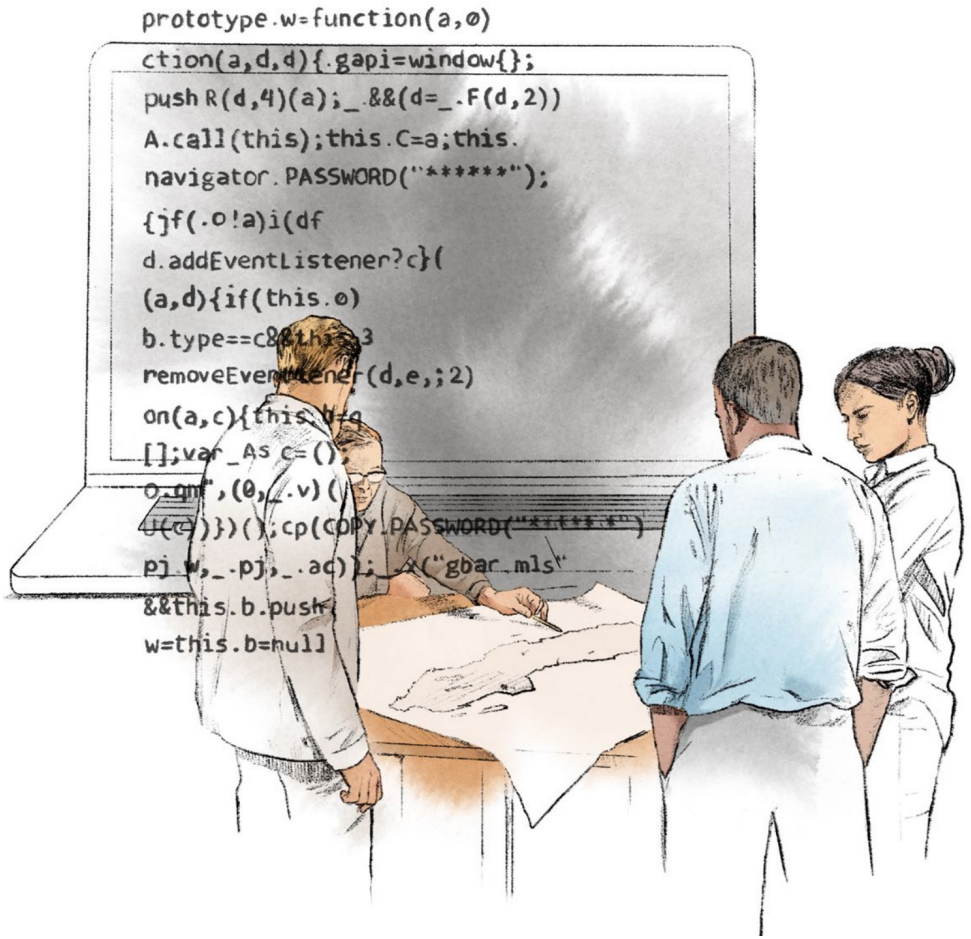
Colonial Pipeline-attacken och samhällets sårbarhet

Attacken mot Colonial Pipeline i USA bidrog till bensinbrist i flera stater i sydöstra USA. Säkerhetsexperten Etay Maor berättar för Voister om bakgrunden till attacken och hur vi bör skydda oss.

– Det finns anledning att tro att det började med phishing-mail, vilket i sig inte skulle vara någon överraskning. Men det är fortfarande väldigt mycket som är oklart kring händelseförloppet, säger Etay Maor, professorsadjunkt vid Boston College och senior director för cybersäkerhetsstrategi på säkerhetsföretaget Cato Networks

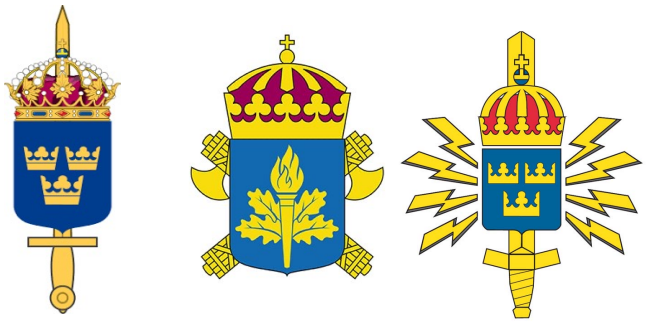
Nytt center stärker svensk cybersäkerhet

Cyberangreppen mot Sverige är reella och omfattande. Som ett led i att stärka Sveriges förmåga och motståndskraft på området beslutade därför regeringen i december 2020 om inrättandet av ett nationellt center för cybersäkerhet. Centret kommer att få **en viktig roll i arbetet med att minska avståndet mellan hot och skydd på cyberområdet.**



Försvarsmakten rustar för cyberkrig – ”digitalt slagfält” Stod klart mars 2020

Nära samverkan



”Varför-filmen”
https://www.youtube.com/watch?v=2EM-dbwkA2Y

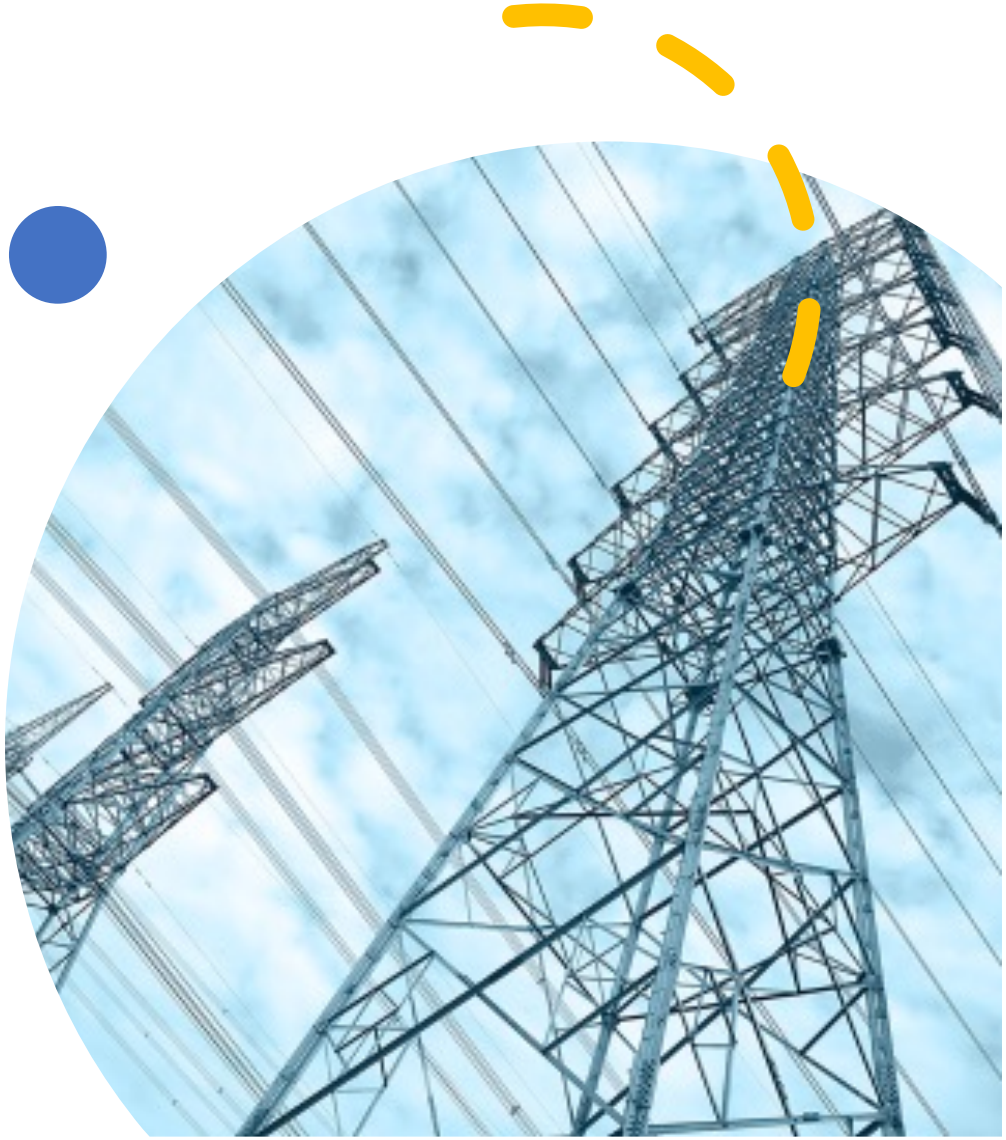
Europeisk lagstiftning

NIS Direktivet

Direktivet ställer krav på säkerhet i nätverk och informationssystem. Reglerna omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster. Dessa leverantörer kan finnas i både privat och offentlig sektor.

- Den svenska NIS-regleringen innebär i korthet krav på informationssäkerhet och incidentrapportering för leverantörer av **samhällsviktiga- och vissa digitala tjänster.** Dessutom har ett antal myndigheter tillsynsansvar i enlighet med regleringen.
- MSB har en bred roll kopplat till regleringen som bland annat innefattar föreskriftsrätt, att samordna det nationella arbetet, motta incidentrapporter, och att utgöra kontaktpunkt gentemot andra europeiska medlemsstater.
- NIS 2 kommer

Du som vill veta mer om den svenska NIS-regleringen kan läsa på MSB:s webbplats: www.msb.se/nis



Ny säkerhetsskyddslagstiftning 1 april 2019

Syftet med den nya lagstiftningen är att tydliggöra kraven på säkerhetsskydd hos utövare av säkerhetskänslig verksamhet – alltså sådan verksamhet som har betydelse för Sveriges säkerhet.

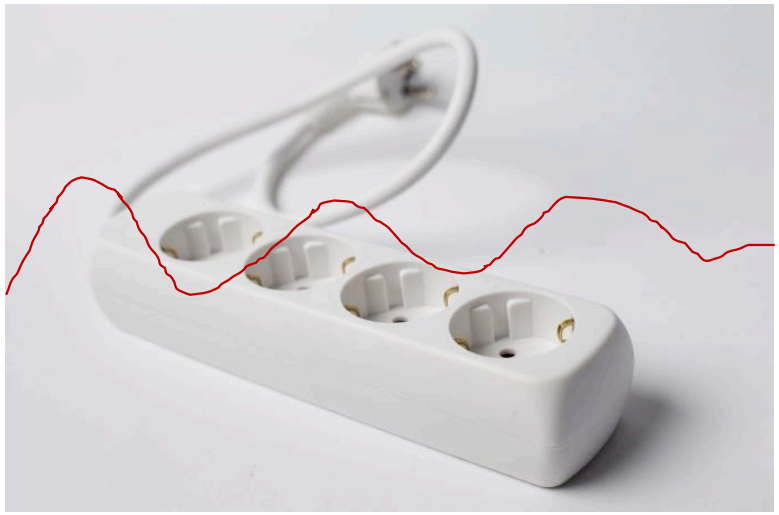
En av de största förändringarna är att lagstiftningen tydligare gäller för alla som bedriver säkerhetskänslig verksamhet, vilket även omfattar enskilda verksamhetsutövare.

En viktig utgångspunkt för den egna organisationens säkerhetsarbete är en analys av den säkerhetskänsliga verksamheten, som sammanställs i en säkerhetsskyddsanalys.

För övrigt kommer den nya lagstiftningen innebära bland annat följande för elföretag:

- Den nya lagstiftningen kommer att innebära högre krav på både fysiskt skydd och IT-säkerhet för lokaler, anläggningar och system som bedöms vara säkerhetskänsliga. Informationssäkerhet…
- Säkerhetsskyddsklassificerade uppgifter delas i den nya säkerhetsskyddslagen upp i fyra klasser (kvalificerat hemlig, hemlig, konfidentiell och begränsat hemlig) ….
- De elföretag som bedriver säkerhetskänslig verksamhet kommer att omfattas av krav på att ingå säkerhetsskyddsavtal med leverantörer… (SUA)
- Reglerna vid användning av utländska leverantörer blir striktare…..
- Säkerhetsskyddsklassificerade uppgifter som kommuniceras till ett system utanför företagets kontroll ska skyddas av kryptografiska funktioner… (FM)
- Svenska kraftnät kommer att under året bjuda in elsektors aktörer till dialog…
- Säkerhetspolisen kommer att ta fram ett antal vägledningar för att tydliggöra kraven i föreskrifterna, bland annat för områden säkerhetsskydd, säkerhetsskyddsanalys och säkerhetsskyddade upphandlingar (SUA)….

Integrera informationssäkerhetsarbetet!



Likheter med:

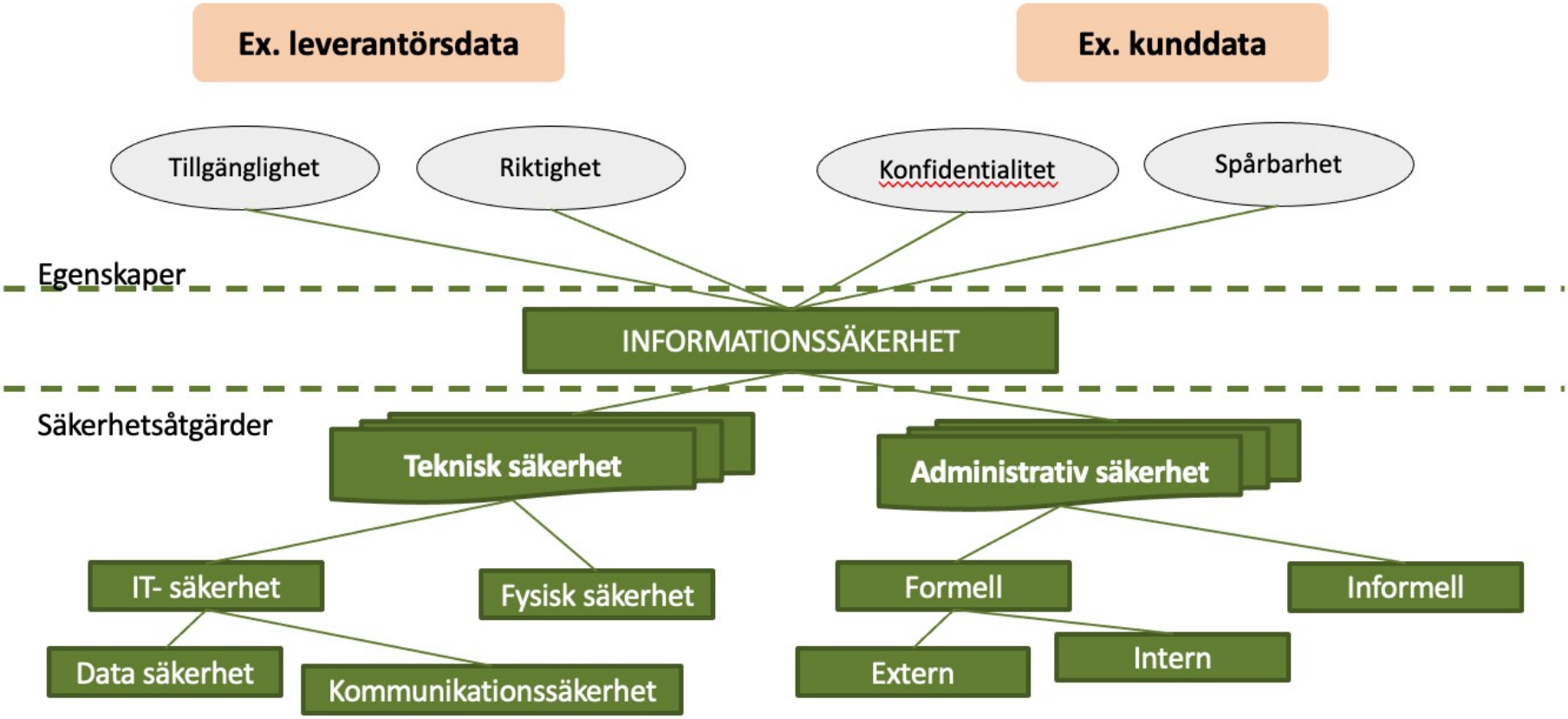
- Kvalitetsledning
  ISO 9001:2015 för hälso- och sjukvården

- Miljöledning
  ISO 14001:2004
  Miljöledningssystem - Krav och vägledning (ISO

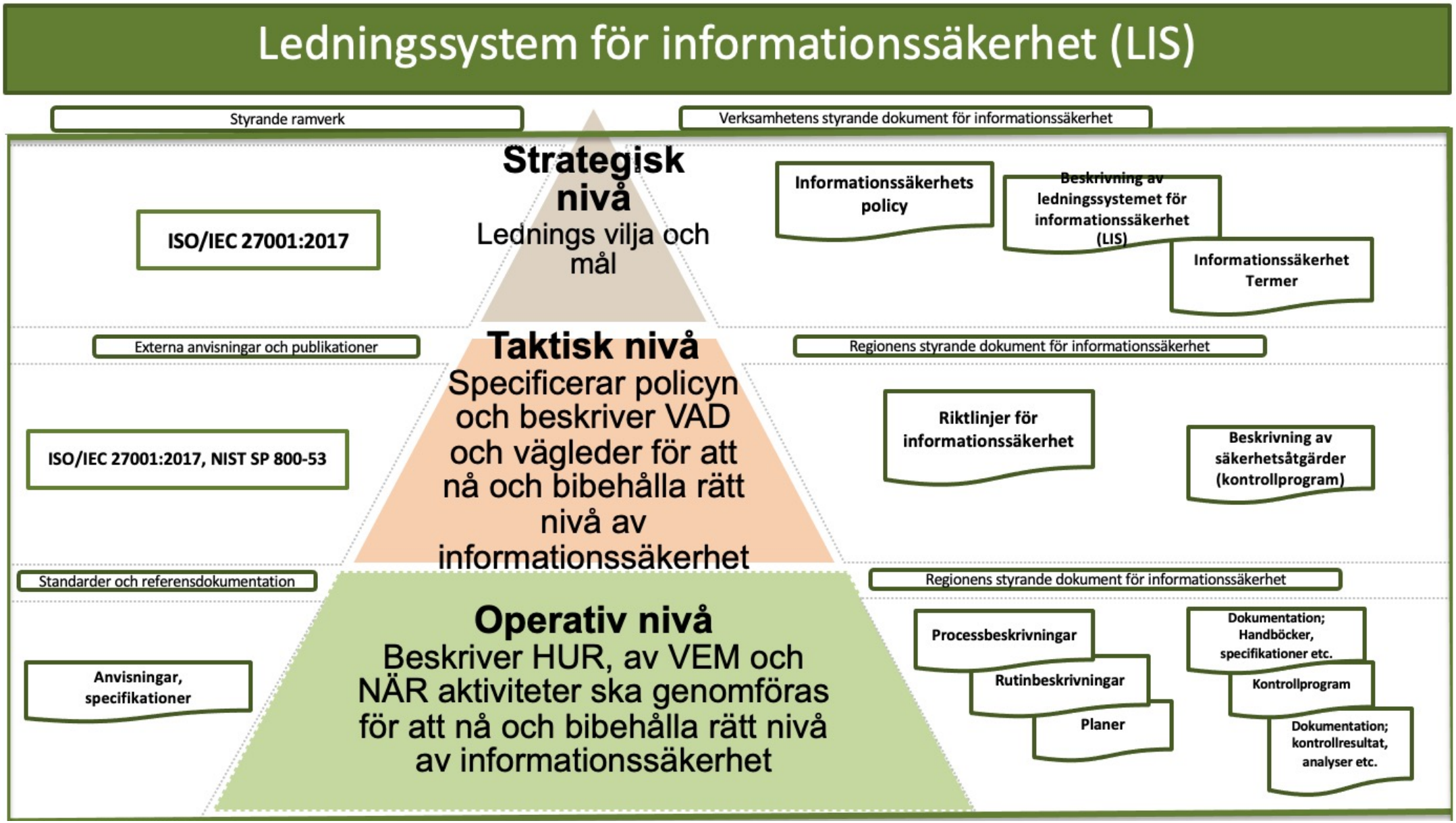
- Arbetsmiljöledning
  ISO 45001:2018
  Ledningssystem för arbetsmiljö

- Informationshantering
  ISO/IEC 27000:2014
  Informationsteknik - Säkerhetstekniker

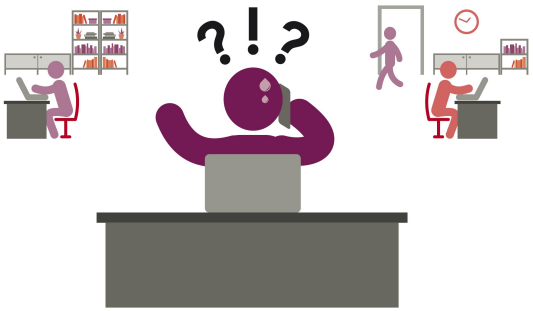
Informationssäkerhetsmodellen



Ledningssystem för informationssäkerhet (LIS)



Tips från MSB



- Metodstöd för systematiskt informationssäkerhetsarbete
- https://www.informationssakerhet.se/metodstodet

- DISA – Digital informationssäkerhetsutbildning
- https://webbutbildning.msb.se/utb/DISA/

Sammanfattning

- Internet 1990 -> Internet of things 2021
- Allvarliga attacker & incidenter har skett och sker
- Myndigheter ställer krav men är också stödjande
- Beprövade standarder för att arbeta systematiskt finns
- Integrera informationssäkerhetsarbetet!