SUHF

Webbseminarium om NIS2

Vad vi vet idag, och hur vi kan förbereda oss

Expertgruppen för säkerhetsfrågor:

Arbetsgruppen kring införandet av cybersäkerhetsreglering

Peter Liljenstolpe, Hans E Andersson

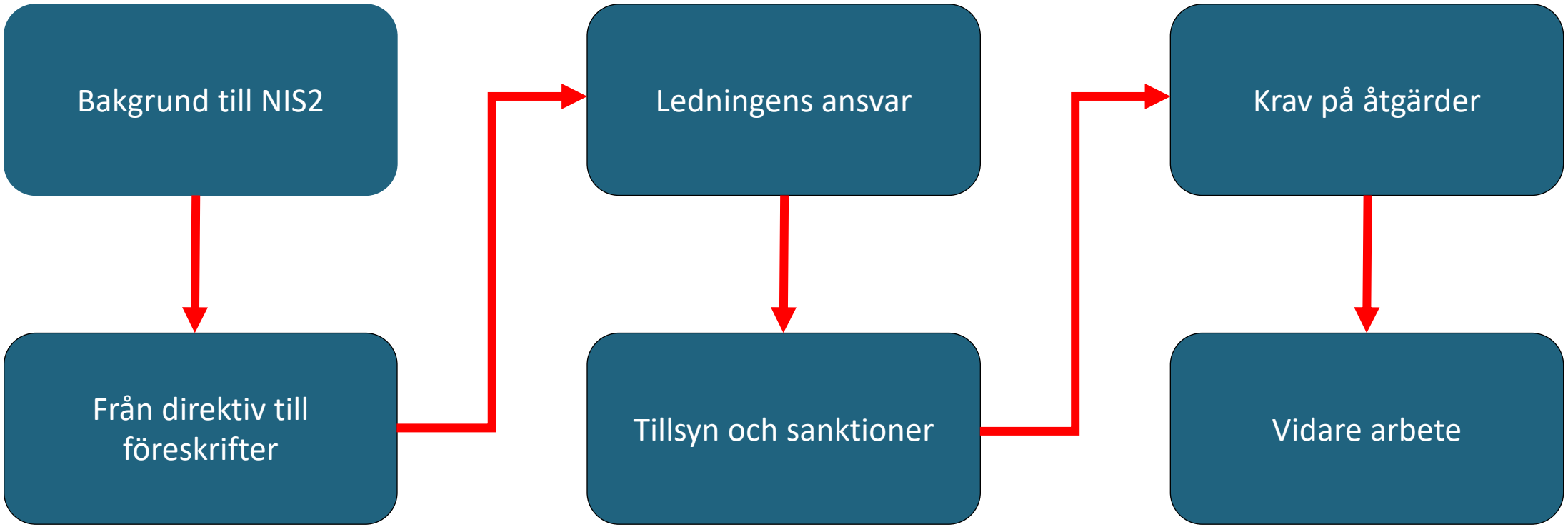
Anders Qvist, Kristoffer Lithén, David Byers

SUHF

Anders Qvist,

CISO Chalmers

SUHF


Bakgrund till NIS2
Från direktiv till föreskrifter
Ledningens ansvar
Tillsyn och sanktioner
Krav på åtgärder
Vidare arbete

SUHF

Bakgrund till NIS2

- NIS (2016) – skapa en gemensam säkerhetsnivå rörande *nätverks- och informationssystem* i unionen
- Säkra den inre marknadens funktion och konkurrenskraft

NIS2 – några skillnader

- Samordnat regelverk, utgår från minimiregler
- Utökar från 7 till 18 sektorer
- Kraven gäller en organisations *hela* verksamhet
- Mer omfattande, proaktiv tillsyn
- Krav på utbildning av ledningen
- Kraftfulla sanktioner

SUHF

Från direktiv till föreskrift...

- NIS2-direktivet (antaget 14 december 2022) – skulle vara implementerat 18 oktober 2024 (!)
- **Utredning** (SOU 2024:18) lämnade delbetänkande våren 2024. Har varit på remiss
- **Proposition** med lagförslag väntas maj 2025
- Riksdagen kommer behandla propositionen *efter sommaren 2025*
- *Gissningsvis* träder **lagen** i kraft i slutet av 2025
- Då även regeringens **förordning** samt MSBs **föreskrifter**

- Sannolikt omfattas samtliga statliga lärosäten samt enskilda lärosäten med examinationsrätt och över viss storlek.

SUHF

Ledningens ansvar

Utredningens förslag

- *Ledningen i enskilda och offentliga verksamheter **ska** genomgå utbildning om riskhanteringsåtgärder och anställda ska erbjudas sådan utbildning. Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om utbildning*
- ”Ledningen”? Utredningen: Offentliga: generaldirektör och de anställda som utövar ledningsfunktion. Enskilda: styrelse och VD
- Flera har reagerat på antydningar till ”skruv o mutter-nivå”..
- Obs! I nuvarande föreskrifter krav på att ledningen är involverad.

Tillsyn och sanktioner

- Utredningen föreslår för offentlig förvaltning länsstyrelsen.
- Stora sanktionseffekter! Avsiktligt *effektivt, proportionell och avskräckande*

Verksamhetsutövare	Högst	Lägst
Väsentlig	Det högsta av 2 procent av den utövarens globala årsomsättning föregående räkenskapsår, eller 10 000 000 euro	5 000 kr
Viktig	Det högsta av 1,4 procent av utövarens globala årsomsättning föregående räkenskapsår, eller 7 000 000 euro	5 000 kr
Offentlig	10 000 000 kr	5 000 kr

- *Sanktion kan även innebära att näringsförbud upprättas för enskilda individer i företagets ledning*

SUHF

Krav på åtgärder - från direktivtexten

Riskanalys och säkerhet i informationssystem	Incidenthantering	Driftskontinuitet	Säkerhet i leveranskedjan	Säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem
Strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet	Grundläggande utbildning i cybersäkerhet	Användning av kryptografi	Personalsäkerhet (åtkomstkontroll och tillgångsförvaltning)	Användning av lösningar för multifaktors-autentisering och säkrad kommunikation

SUHF

Vidare arbete

- Utgå från egna förutsättningar
- Konkret från *SH, MDU, LiU*

SUHF

Södertörns högskola

Hans E Andersson, förvaltningschef

SUHF

Södertörns högskola

- Var är vi i relation till nuvarande regelverk?
  - MSBs *Cybersäkerhetskollen*
    - Ej räkna poäng, utan som ett medel att bedöma sin egen organisation
- Fick ordning på systematik; årlig avrapportering till rektor med mera.
  - Kollektivt arbete
  - Vissa stödfunktioner har delat ansvar, men tillräcklig tydlighet

SUHF

Ett generellt problem: Hur få forskare att informationsklassa forskningsprojekt?

- Försöka undvika begreppen "konfidentialitet", "riktighet" och "tillgänglighet"
- Fatta ett generellt beslut om vissa klassningar ("information om känsliga personuppgifter har nivå 3”)
- Gör det obligatoriskt med datahanteringsplan
- Skapa konkreta frågor i datahanteringsplanen
  - "Finns känsliga personuppgifter?” ”Om ’ja’ – lagra din data på följande platser”
- Utveckla diarieföring så lätt hitta om information med högt skyddsvärde

SUHF

Sammanfattningsvis

- Var är ni i relation till dagens föreskrifter? Ta det därifrån
- En bit i taget; plötsligt har det gått två år och ni har kommit långt
- Forskarna måste och vill agera informationssäkert, men ägna en extra tanke åt hur ni kan begränsa och konkretisera de överväganden de måste göra

SUHF

Mälardalens universitet

Kristoffer Lithén
Informationssäkerhetssamordnare

SUHF

Hur har vi gjort på MDU?

- Lagt fokus på att informera om kommande lag
  - Ledningens genomgång och ledningens uppföljande genomgång
  - Universitetsstyrelsemöten
- GAP-analys
    - MSBFS
    - ISO27000
    - NIS2-direktivet
    - Nya regler om cybersäkerhet
- Åtgärdsplan för riskhanteringsåtgärder

SUHF

Åtgärder

- Riskhanteringsåtgärder från ett allriskperspektiv
  - Röd tråd
- Säkerhetsåtgärder för att skydda informationssystem
  - Lista över viktigaste systemen
  - Ramverk för systemförvaltning
  - Säkerhetsåtgärder
- Process för hantering och rapportering av cybersäkerhetsincidenter
  - Revidera och komplettera

SUHF

Ytterligare åtgärder

- Utbildning av anställda
  - Junglemap (Nanolearning) sedan 2024
  - Utbildning av universitetsledningen planeras
- Säkerhet i leveranskedjan
  - Inventera avtalsdatabasen
  - Systemägare har viktig roll
  - Från behov till förvaltning
- Ramverk för informationsförvaltning

SUHF

Sammanfattning

- Min bedömning: Vi behöver agera, oavsett gällande eller kommande föreskrifter
- Gott samarbete med IT
- Förståelse för påverkan, ledning och verksamheten

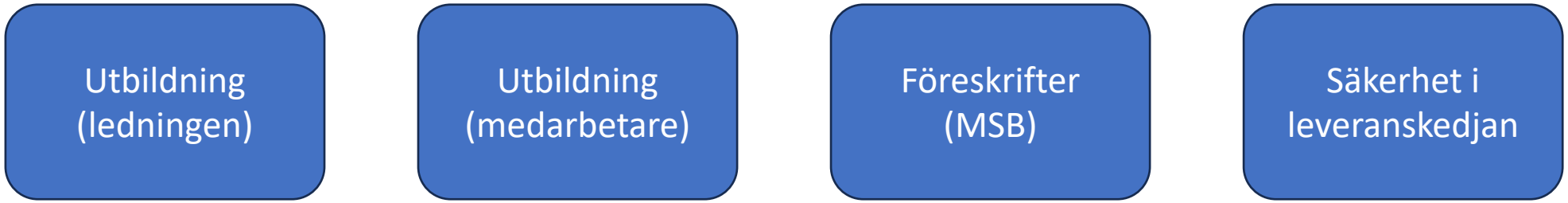
SUHF

Linköpings universitet

David Byers
Enhetschef

Hur agerar Linköpings universitet?

- Utgår från det vi **vet**, är **rätt säkra på**, eller borde göra ändå
- Avvakta med osäkra, stora, och kostsamma åtgärder

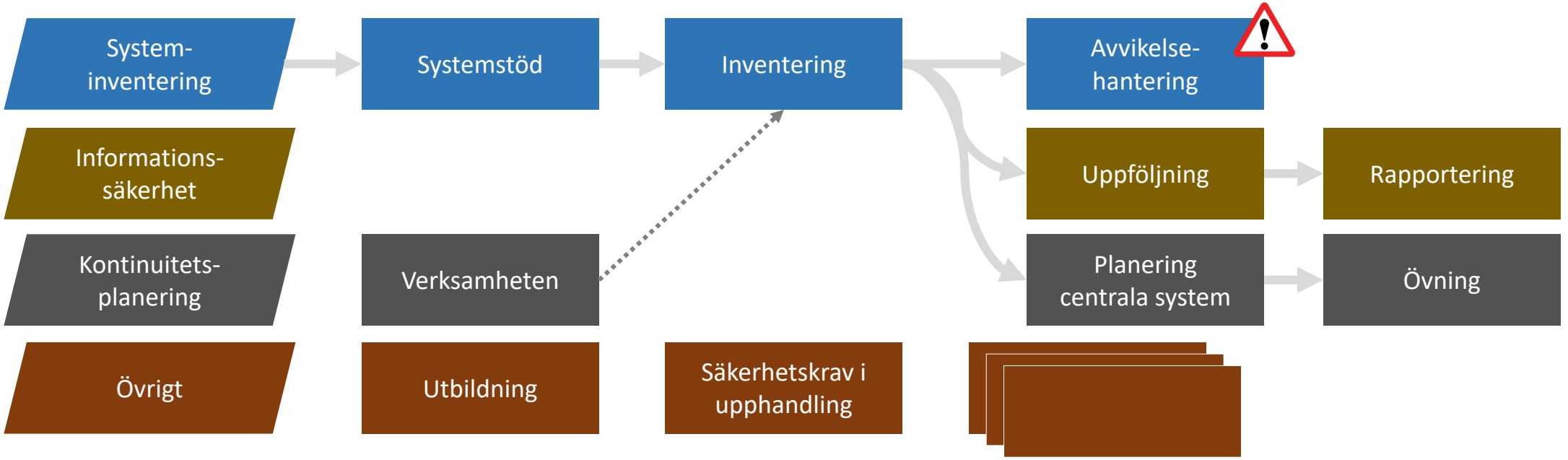


- Begränsa fokus
  - IT – NIS 2 är inte bara IT, men IT är en stor del
  - Det systematiska informationssäkerhetsarbetet

SUHF

Analys av nuläget och förutsättningarna

- Gap-analyser mot flera olika regelverk och standarder
  MSBFS 2020:6, MSBFS 2020:7, MSBFS 2020:8, PMFS 2022:1, NIS 2, ISO 27001, ISO 27002, NIST SP 800-171, (NIST SP 800-53)
- Identifiera avvikelser och åtgärder för att hantera avvikelserna



SUHF

Utbildning

- **Syftar till att möta utbildningskraven i direktivet**

- Anpassning av DISA från MSB
  - Avsett att användas i grupp, t.ex. på arbetsplatsträffar
  - Kompletterat med lokala anpassningar

- Kommersiellt utbildningsmaterial (Complorer)
  - Integrerat i LiU:s internutbildningsplattform
  - Inköpt material med lokala kompletteringar
  - Erbjuds till alla anställda **och studenter**

SUHF

Systeminventering

- **Syftar till att möta så många föreskriftskrav som möjligt**

- Utveckling av systemstöd inom ramen för ITCF
- Identifiering av alla **informationssystem** och **systemägare**
- Dokumentation av beroenden och andra centrala aspekter
- Systemspecifika gap-analyser mot interna och externa regelverk
- Åtgärdsplaner för att hantera avvikelser

SUHF

Säkerhet i upphandlingar

- **Syftar till att möta krav på säkerhet i leveranskedjan**

- Verktyg för urval av krav baserat på informationsklass och objekttyp
- Utökade krav på leverantören
  - Krav motsvarande kraven som ställs på LiU i MSBFS 2020:7
  - Utökade krav på leverantörens cybersäkerhet
- Utökade krav på beställaren
  - Krav på dokumentation av beslut att utesluta krav
  - Krav på dokumentation av skäl till att utesluta krav

SUHF

Sammanfattning

- Bevaka situationen
- Analysera läget utifrån nuvarande reglering
- Identifiera aktiviteter som kan göras nu
- Identifiera aktiviteter som är en förutsättning för annat
- Avvakta utvecklingen men var beredd att agera

- **Delta i MSB:s samverkan i SNITS kring föreskrifterna**

  https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/kurser-och-natverk-inom-informationssakerhet/natverk-om-informationssakerhet-for-offentliganstallda/

Avslutning

Mejla gärna önskemål på teman för fler seminarier!

Lars.alberius@suhf.se

Kort om kommande webbinar...