NIS2 – träffas ni av de utökade cybersäkerhetskraven?

Agnes Hammarstrand & Louise Sundström
Från Advokatfirman Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Vilka är vi?

- Specialister inom IT/tech och digital juridik
- Delphi är en advokatbyrå med erkända specialister inom de flesta av affärsjuridikens områden
- Stort team inom Tech, GDPR, IT-juridik och e-handel
- Tveka inte att slå en signal eller maila om du har någon fråga eller vill diskutera samarbete!
- Missa inte vår techblogg: https://www.delphi.se/en/tech-blog/

BG Institute
EN DEL AV BLENDOW GROUP

Delphi

Bakgrund och NIS-lagen idag

BG Institute
EN DEL AV BLENDOW GROUP

Bakgrund

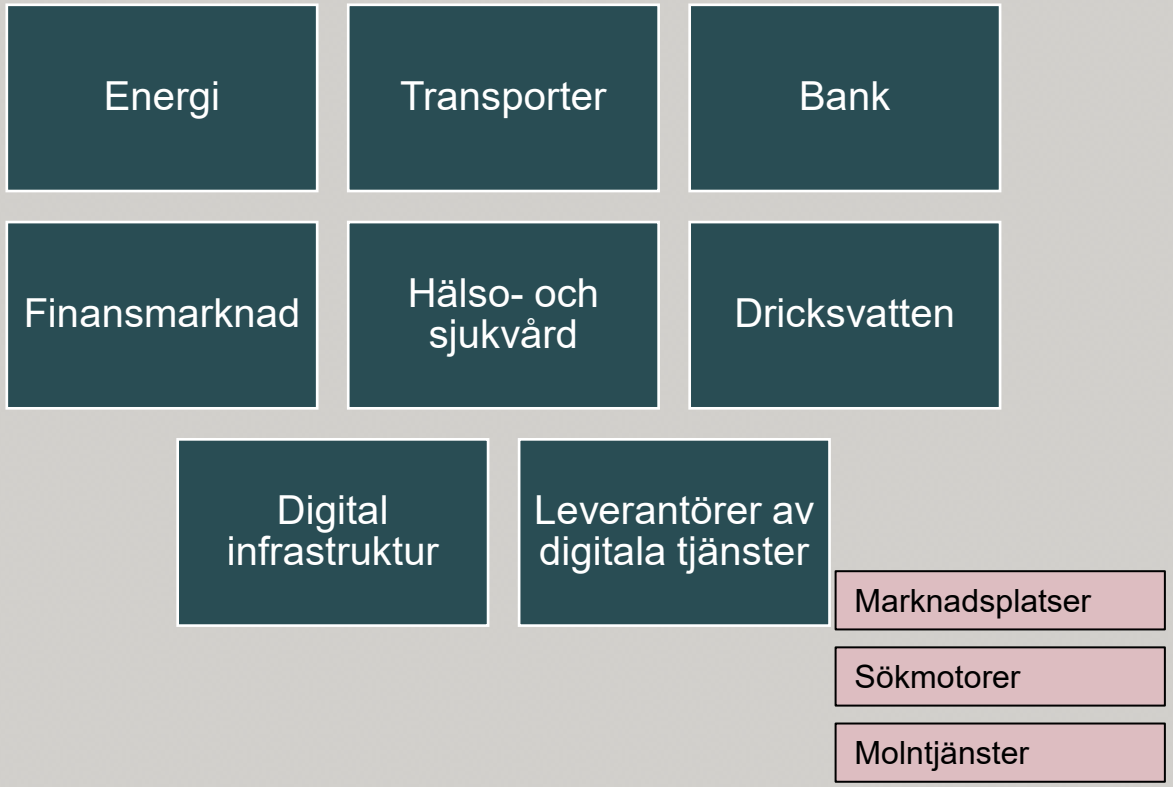
- NIS – Network and Information Systems
- Fler, mer omfattande och allvarligare incidenter som dataintrång, bedrägerier och spridning av skadlig kod
- Bristande informationssäkerhet kan få stora konsekvenser för samhället
- Idag – NIS1
  - I Sverige: NIS-lagen ”Lag om informationssäkerhet för samhällsviktiga och digitala tjänster” från 2018
- Snart kommer NIS2

BG Institute
EN DEL AV BLENDOW GROUP

Delphi

NIS1 - Lagen idag

- Gäller leverantörer av ”samhällsviktiga tjänster” eller (vissa) digitala tjänster
- Såväl privata som offentliga aktörer
  - Samhällsviktiga tjänster
  - Digitala tjänster i vissa fall
- Under vissa förutsättningar och med flera undantag
- Lagen övervakas av MSB samt flera sektorsspecifika myndigheter



NIS1 – Vilka krav ställs idag?

- Innehåller krav på systematiskt och riskbaserat infosäkerhetsarbete
- Krav på att rapportera incidenter
- Även krav på att säkerställa att leverantörer följer kraven – ”NIS-avtal” i upphandlingar och avtal

NIS2

BG Institute
EN DEL AV BLENDOW GROUP

Nu kommer NIS2

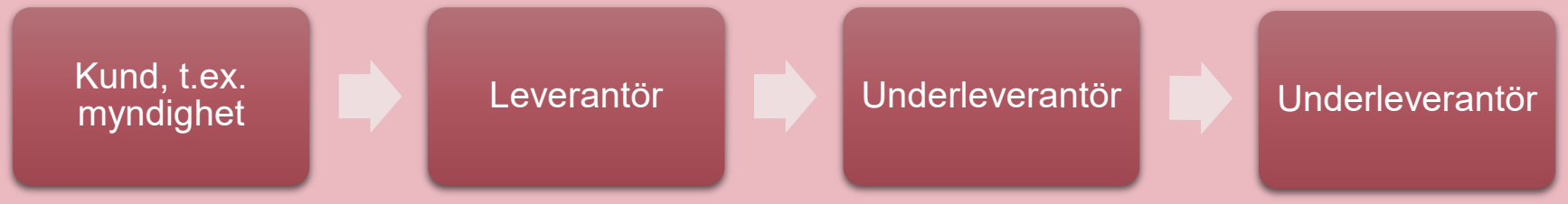
- EU har en ny cybersäkerhetsstrategi – vill skapa en högre och jämnare nivå
- Anger en miniminivå – medlemsländer som Sverige kan anta striktare reglering
- Riktar sig mot alla aktörer (”entiteter”) som fyller viktiga samhällsfunktioner
- Berör företags och myndigheters policyer, processer och strategier kring cyber- och informationssäkerhet

BG Institute
EN DEL AV BLENDOW GROUP

Delphi

Viktiga nyheter i korthet

- Fler sektorer och aktörer omfattas
- Cybersäkerhet blir mer tydligt ett ansvar för ledningen – ska kunna ställas till svars
- Strängare krav och högre sanktioner
- Ökade krav på incident- och riskhanteringsåtgärder – fokus på standarder, t.ex. ISO
- Verktyg för att kunna samarbeta effektivt mellan myndigheter i varje EU-land
- Särskilt fokus på sårbarhet i leverantörskedjor



NIS2 - status

- Ska börja tillämpas **18 oktober 2024**
- EU-direktiv som ska bli svensk lag – utredning tillsatt
- Hur svenska lagen kommer se ut och vilka myndigheter som har tillsyn är inte klart

BG Institute
EN DEL AV BLENDOW GROUP

Delphi

Sverige utreder just nu flera frågor

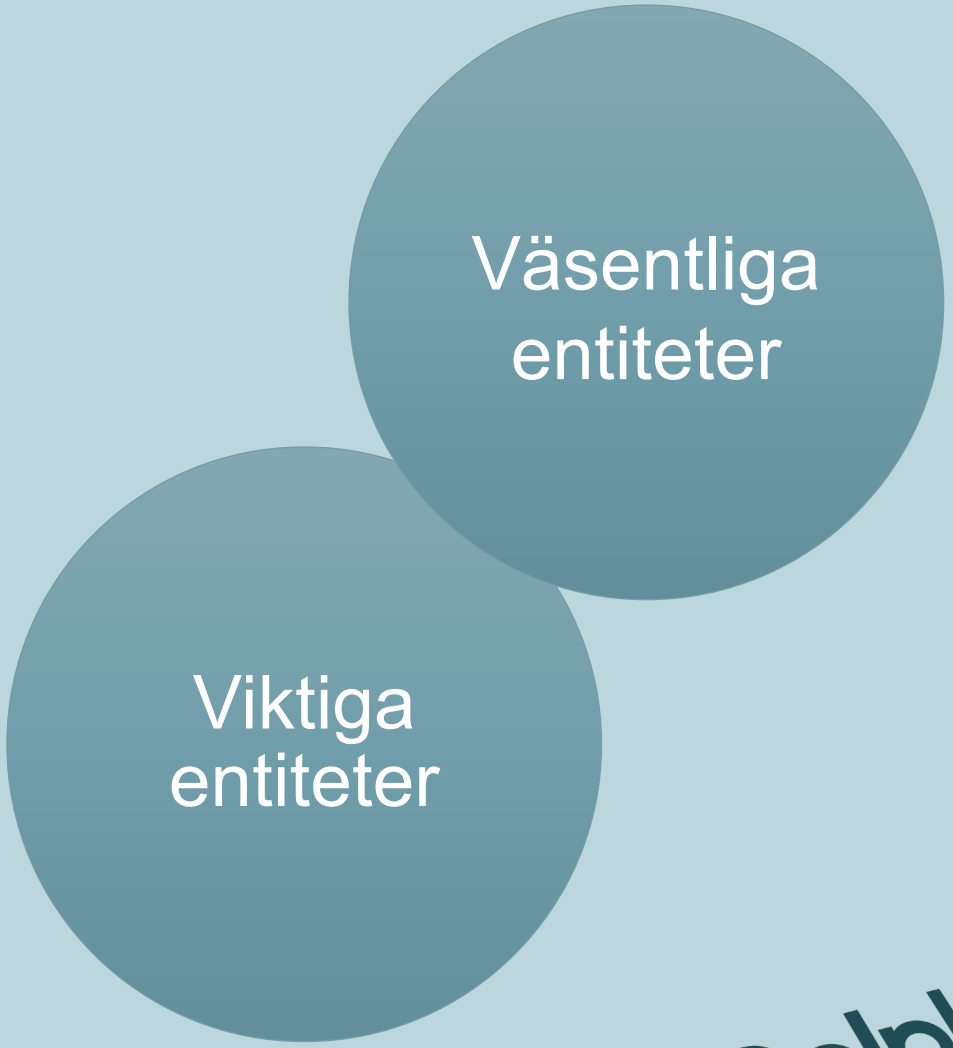
- Ska kommuner, universitet och högskolor omfattas?
- Behöriga myndigheter och deras befogenheter
- Hur hårda kraven ska vara enligt svensk lag
- Sanktioner
- Och en del annat…
- Ska redovisas senast 23 februari 2024

För vilka gäller NIS2?

BG Institute
EN DEL AV BLENDOW GROUP

Vilka omfattas?

- Delas in i viktiga och väsentliga entiteter
- Många fler sektorer än tidigare
- De som omfattas listas tydligt
  - Bilaga I – högkritiska sektorer (väsentliga)
  - Bilaga II – andra kritiska sektorer (viktiga)
- Entitetens storlek har betydelse - företag med mindre än 50 anställda och under 10 MEUR i omsättning undantas normalt
- Ska bedriva verksamhet i eller rikta sig till EU



BG Institute
EN DEL AV BLENDOW GROUP

Delphi

Nya sektorer

BG Institute
EN DEL AV BLENDOW GROUP

Delphi

Skillnader?

De största skillnaderna mellan väsentliga och viktiga entiteter är:

- Sanktionsavgifternas storlek
  - **Väsentliga**: 10 000 000 EUR eller 2 % av total global årsomsättning
  - **Viktiga**: 7 000 000 EUR eller 1,4 % av total global årsomsättning
- När och hur de granskas:
  - **Väsentliga**: granskas ”proaktivt”
  - **Viktiga:** granskas ”reaktivt”

BG Institute
EN DEL AV BLENDOW GROUP

Delphi

Ett axplock av de nya kraven

BG Institute
EN DEL AV BLENDOW GROUP

Riskhanteringsåtgärder

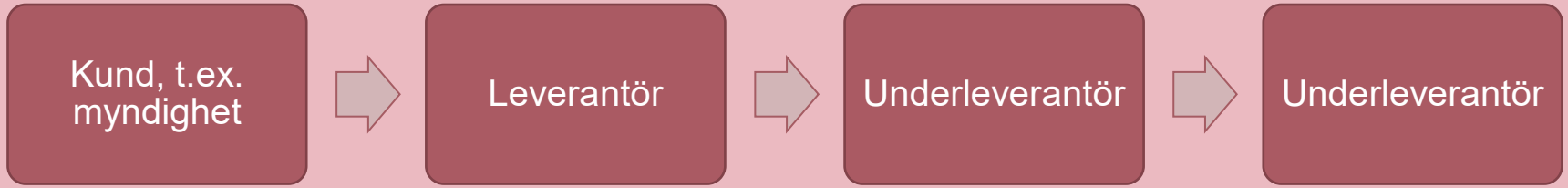
- Stort ansvar för systematiskt arbete
- ”**Allriskansats**” utifrån verksamhetens förutsättningar – är verksamheten t.ex. beroende av nätverks- och informationssystem?
- Ännu inte helt tydligt exakt vad kraven kommer innebära i detalj

BG Institute
EN DEL AV BLENDOW GROUP

Delphi

Krav på att beakta hela ”kedjan”

- Säkerhet i hela leveranskedjan
- Köp, utveckling och underhåll av nätverks- och informationssystem
- Bedöm övergripande kvaliteten och motståndskraften hos leverantörer, produkter och tjänster
- Riskhantering och cybersäkerhet i avtal



Skyldighet att rapportera incidenter

- Krav att rapportera incidenter till MSB
- Samma krav för alla - ska rapportera *betydande incidenter*
  - Har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsten eller ekonomiska förluster
  - Har påverkat eller kan påverka andra fysiska eller juridiska personer
- Informera kunder om incidenten sannolikt inverkar negativt på kundens användning
  - Vid betydande cyberhot även informera om vad kunden kan göra
- Myndigheterna ska samråda och bistå

Rapportering i steg

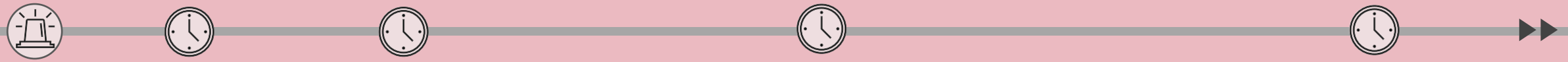
Tidig rapport

Incident-anmälan

Delrapport

På begäran av CSIRT- eller behörig myndighet

Slutrapport



0 h **24 h** **72 h** **1 månad**

Incident upptäcks

BG Institute
EN DEL AV BLENDOW GROUP

Delphi

Jämförelse annan lagstiftning

GDPR	• Gäller alla om personuppgifter behandlas • Krav att rapportera till IMY inom 72 timmar • Krav att i vissa fall krav att informera individer
Säkerhetsskyddslagen och förordningen	• Gäller den som bedriver säkerhetskänslig verksamhet. • Krav att skyndsamt anmäla incidenter i flera fall, t.ex. om säkerherhetsklassificerade uppgifter har röjts, IT-incidenter med betydelse för säkerhetskänslig verksamhet, m.m.
MAR	• Krav för Bolag noterade på börs eller som har lämnat in ansökan om att bli börsnoterade • Innebär Krav att i som huvudregel offentliggöra för allmänheten att incident skett
Finansinspektionen	• Krav för banker, betaltjänstinstitut, registrerad betaltjänstleverantör, institut för elektroniska pengar • Krav att rapportera allvarliga operativa incidenter och säkerhetsincidenter i betaltjänstverktyget till finansinspektionen

BG Institute
EN DEL AV BLENDOW GROUP

Delphi

Tillsyn och sanktioner

BG Institute
EN DEL AV BLENDOW GROUP

Nytt fokus på ledningsgruppen

- Ledningen ska godkänna riskhanteringsåtgärderna för cybersäkerhet och övervaka genomförandet
- Ledningen kan ställas till svars för överträdelser
- Medlemmarna i ledningen ska genomgå utbildning
  - För att kunna identifiera risker och bedöma riskhanteringspraxis
- Uppmuntras att regelbundet erbjuda sådan utbildning till sina anställda

BG Institute
EN DEL AV BLENDOW GROUP

Delphi

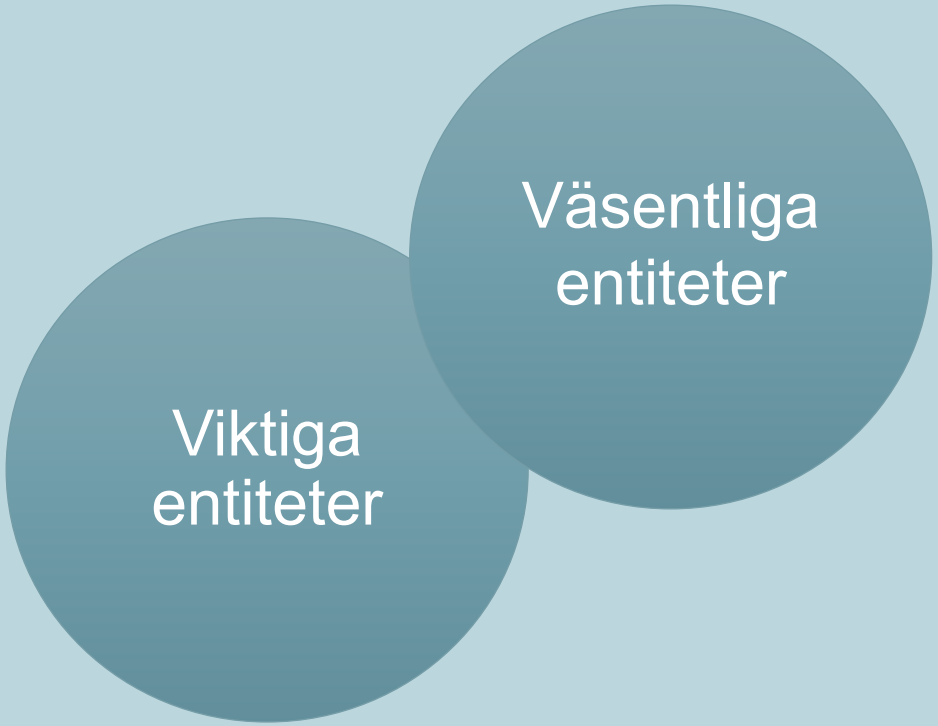
Tillsyn

- Tillsynsmyndigheterna ska agera **proaktivt** eller **reaktivt** beroende på typ av entitet
- Åtgärder som är **effektiva, proportionella** och **avskräckande**
- Vad får myndigheterna göra?
  - Inspektioner och slumpvisa kontroller
  - Regelbundna och riktade säkerhetsrevisioner och säkerhetsskanningar
  - Även revision i efterhand om incident
  - Begära information och bevis på att entiteten följer reglerna

Mer tillsyn och högre sanktioner

Varierar beroende på typ av aktör

- Sanktionsavgifternas storlek
  - **Väsentliga**: 10 000 000 EUR eller 2 % av total global årsomsättning
  - **Viktiga**: 7 000 000 EUR eller 1,4 % av total global årsomsättning
- När och hur de granskas:
  - **Väsentliga:** granskas ”proaktivt”, genom exv. inspektioner, revisioner och begäranden om information
  - **Viktiga:** granskas ”reaktivt”, dvs. i efterhand (efter klagomål eller incident)



Utöver sanktioner även risk för

- Varning och reprimand
- Bindande instruktioner
- Kräva att riskhanteringsåtgärder eller rapporteringsskyldighet säkras inom viss tid
- Avhjälpa brister inom en viss tid
- Om entiteten inte vidtar åtgärderna – certifieringar eller auktorisationer tillfälligt upphävda, för hela eller delar av verksamheten
- Ledningsförbud för juridiskt ombud samt för VD (om väsentlig entitet)

Avslutning

BG Institute
EN DEL AV BLENDOW GROUP

Checklista – vad kan ni göra redan nu?

- ✓ Undersök om ni träffas av NIS
- ✓ Leverantör? Fundera över om er kundgrupp träffas
- ✓ Kartlägg vilka krav ni omfattas av
- ✓ Implementera tekniska och organisatoriska åtgärder och rutiner
- ✓ Arbeta löpande med cybersäkerhet!
- ✓ Håll er uppdaterade kring svenska lagen

BG Institute
EN DEL AV BLENDOW GROUP

Delphi

Delphi team

Louise Sundström

Senior Associate / Advokat

E-mail: louise.sundstrom@delphi.se
Mobil +46 709 25 26 14

Agnes Hammarstrand

Partner / Advokat

E-mail: agnes.Hammarstrand@delphi.se
Mobil: +46 730 83 50 70

BG Institute
EN DEL AV BLENDOW GROUP

Delphi

Nya direkt kring nätverks- och informationssäkerhet – NIS2

Agnes Hammarstrand & Louise Sundström, Stockholm den 16 maj

Till dig som deltog på dagens webbinarium erbjuder vi nu 20 % rabatt på vår uppföljningskurs

Boka din plats senast den 20 oktober för att ta del av erbjudandet

Använd rabattkod: **nis20**

BG Institute
EN DEL AV BLENDOW GROUP

Låt oss veta vad du tycker!

Vi skulle uppskatta om du tog 30 sekunder till att fylla i vår utvärdering

Jag är nöjd med webbinariet. *

1 = stämmer inte alls. 5 = stämmer helt.

- ○ 5
- ○ 4
- ○ 3
- ○ 2
- ○ 1

Jag skulle kunna tänka mig en fördjupningskurs inom samma ämne. *

- ○ Ja
- ○ Nej

Övriga kommentarer om webbinariet.

Ditt svar

Länk till utvärderingen finner du i chatten.

BG Institute
EN DEL AV BLENDOW GROUP