NIS2, vad betyder det för support-verksamheten och hur förbereder vi oss?

UNDERRUBRIK

BiTA - Vi gör skillnad, vi förenklar förändring, vi levererar Operativ Excellens!

Vad är NIS2?

EN NY SVENSK LAG

- NIS2 (Network and Information Security 2) är ett EU-direktiv som syftar till att stärka organisationers motståndskraft mot cyberhot. NIS2 ersätter NIS som kom 2016 och vann laga kraft 2018.
- NIS2 gäller i hela EU och ett större antal olika organisationer kommer att påverkas än av NIS
- NIS2 är ett direktiv vilket innebär att varje medlemsstat skall inkludera kraven i sina nationella lagar. I Sverige kommer lagen att heta *Cybersäkerhetslagen*
- NIS2 kom i december 2022 vilket innebar att medlemsstaternas lagar skulle vara klara senast december 2024…

Dokumentets struktur

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555

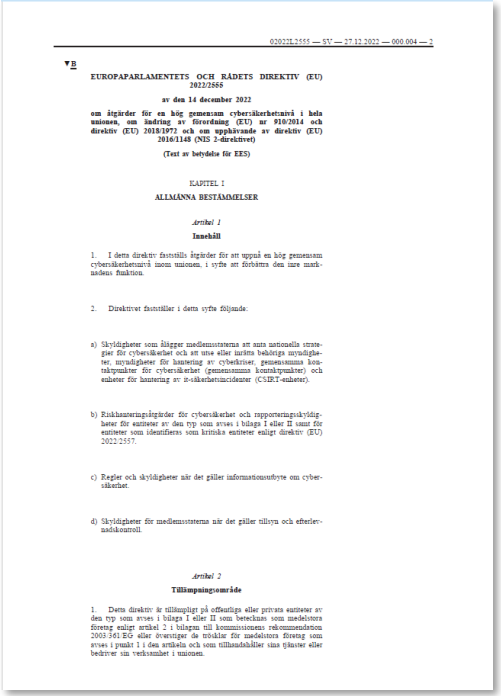
Dokumentet är uppdelat i kapitel där varje kapitel består av en eller fler artiklar

Innehåll per kapitel:

1. Allmänna bestämmelser (Artikel 1-6)
2. Samordnade ramverk för cybersäkerhet (Artikel 7-13)
3. Samarbete på unionsnivå och på internationell nivå (Artikel 14-19)
4. Åtgärder för riskhantering och rapporteringskrav för cybersäkerhet (artikel 20-25)
5. Jurisdiktion och registrering (Artikel 26-28)
6. Informationsutbyte (Artikel 29-30)
7. Tillsyn och efterlevnadskontroll (Artikel 31-37)
8. Delegerade akter och genomförandeakter (Artikel 38-39)
9. Slutbestämmelser (Artikel 40-46)

Bilagor:

1. Högkritiska sektorer
2. Andra kritiska sektorer
3. Jämförelsetabell



02022L2555 — SV — 27.12.2022 — 000.004 — 2

▼B

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555

av den 14 december 2022

om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet)

(Text av betydelse för EES)

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll

1. I detta direktiv fastställs åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen, i syfte att förbättra den inre marknadens funktion.

2. Direktivet fastställer i detta syfte följande:

a) Skyldigheter som åläggermedlemsstaterna att anta nationella strategier för cybersäkerhet och att utse eller inrätta behöriga myndigheter, myndigheter för hantering av cykerkriser, gemensamma kontaktpunkter för cybersäkerhet (gemensamma kontaktpunkter) och enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter).

b) Riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter för entiteter av den typ som avses i bilaga I eller II samt för entiteter som identifieras som kritiska entiteter enligt direktiv (EU) 2022/2557.

c) Regler och skyldigheter när det gäller informationsutbyte om cybersäkerhet.

d) Skyldigheter för medlemsstaterna när det gäller tillsyn och efterlevnadskontroll.

Artikel 2

Tillämpningsområde

1. Detta direktiv är tillämpligt på offentliga eller privata entiteter av den typ som avses i bilaga I eller II som betecknas som medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG eller överstiger de tröskler för medelstora företag som avses i punkt 1 i den artikeln och som tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen.

Utbildning i cybersäkerhet

Så här står det:

- ”Medlemsstaterna ska uppmuntra väsentliga och viktiga entiteter att regelbundet erbjuda liknande utbildning till sina anställda för att de ska få tillräckligt med kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på de tjänster som tillhandahålls av entiteten.”
- grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,

Det här betyder det:

- Två olika utbildningar skall genomföras:
  1. Grundläggande utbildning rörande cybersäkerhet för alla anställda i syfte att minimera risker för attacker som kan genomföras på grund av oaktsamhet
  2. Djupare utbildning till IT personal rörande cybersäkerhet
- Det är viktigt att utbildningen genomförs minst årligen då utvecklingen på området är snabb

Det här gör vi:

- Då det än så länge inte finns någon utbildning tillhandahållen av tillsynsorgan eller motsvarande gäller det att själv hitta relevant utbildning. Det värsta man kan göra är att vänta!
- Här är några länkar:
  - https://metodstod-informationssakerhet.msb.se/
  - https://www.sis.se/iso27001/dettariso27001/
  - https://www.cert.se/

Kontinuitet – Två delar

HUR SKA VI ARBETA?

Återskapande (IT)

- IT ansvara för att det finns återställningsplaner på hela infrastrukturen
- Planerna skall vara tidsatta och testade. Återskapandetider meddelas verksamheterna
- I dialog med verksamheterna skall en turordning av IT-tjänsternas återskapande tas fram
- Planerna skall testas (minst årligen) och vid behov uppdateras
- En konsekvensanalys såsom beskriven i ISO 22301 rekommenderas som ett initialt arbetssätt

Kontinuitet (IT och övrig verksamhet)

- All verksamhet har till ansvar att skapa planer på alternativa arbetssätt då IT-stödet inte längre är tillgängligt
- Utgår från att respektive verksamhet fokuserar på att kunna genomföra sina grunduppdrag
- Varje verksamhet skall även uppskatta under hur lång tid manuella rutiner kan användas innan risk för att verksamheten inte kan fullgöra sitt uppdrag uppstår
- Planerna för alternativa arbetssätt skall testas minst årligen och vid behov uppdateras

Planer för återskapande samt alternativa arbetssätt skall givetvis vara åtkomliga då all IT ligger nere

På vilket sätt påverkas supporten av kraven?

ARTIKEL 21:2

a) strategier för riskanalys och informationssystemens säkerhet,

b) incidenthantering

c) driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, och krishantering,

d) säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess direkta leverantörer eller tjänsteleverantörer,

e) säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation,

f) strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet,

g) grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,

h) strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering,

i) personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning,

j) användning inom entiteten, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem.

Länkar

- MSB
  - Kort om NIS2
  - Föreskrift om rapportering av it-incidenter
- EU
  - NIS2 direktivet från EU
- Regeringen
  - Utredningen
- CIS – Center for Internet Security
  - Controls v8