dansk·it

GoLearn
part of eduhouse

Agenda

- Hvorfor nu lige NIS2
- Hvem dækker NIS2
- Ledelsesansvar
- Hvad siger jeres kollegaer
- Cyber awareness certificering fra GoLearn
- Afrundning og spørgsmål

Flemming Serritzlew

Head of
Customer Success, GoLearn

Kontakt på:

fs@golearn.dk
linkedin.com/in/flemming-serritzlew

Det startede med NIS 1

"Direktiv om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen"

- **Det første direktiv blev vedtaget i 2016**
  - Trådte i kraft omkring samme tid som GDPR i maj 2018
  - Men det blev måske lidt glemt
  - Stiller krav til (risikobaseret) sikkerhed hos udvalgte sektorer, der leverer kritisk infrastruktur (f.eks. forsyning, transport, tele- og internet, mv.)

  - **Formål:** At sikre et højt niveau af cybersikkerhed på tværs af medlemsstaterne

  - **I praksis:** Er blevet implementeret og håndhævet (meget!) forskelligt på tværs af EU-lande og en rimelig vag tilgang i Danmark

NIS 2

Primære formål

- Harmonisering!
- Udvidelse af omfattede sektorer (dog undtagelse for små virksomheder)
- Flere og mere konkrete (sikkerheds)krav
- Mere håndhævelse, herunder bøder og ledelsesansvar

Væsentlige enheder

Energi – forsyning, distribution, transmission og salg af energi (el, fjernvarme og -køling, olie, gas og brint)

Transport – sø og luftfart, jernbane og vejtransport

Bank og finansiel markedsinfrastruktur – bankvæsen, finansielle markedsinfrastrukturer, handel og børser

Sundhed – forskning, produktion, udbydere og fremstillere af medicinsk udstyr

Drikkevand og spildevand – primærleverandører og -distributører

Digital infrastruktur – internetudvekslingspunkter, DNS-udbydere, TLD-navneregistre, cloudcomputing, datacentertjenester, tillidstjenesteudbydere, mfl.

IKT-tjenester (B2B) – udbydere af administrerende tjenester og sikkerhedstjenester

Offentlig forvaltning – statslige og regionale forvaltninger

Rummet – infrastruktur til rumtjenester

Vigtige enheder

Post- og kurerservice – postvæsen og kurertjenester

Affaldshåndtering

Kemiske produkter – fremstilling, produktion og distribution

Fødevarer – produktion, forarbejdning og distribution

Fremstilling og produktion – medicinsk udstyr, computere, elektronik, optisk udstyr, elektrisk udstyr, maskineri, køretøjer, transportudstyr, mv.

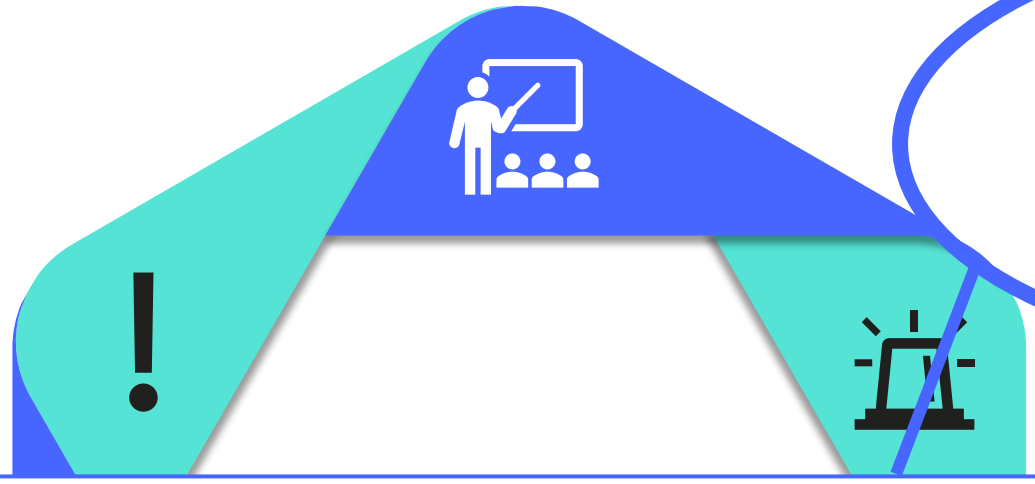
Digitale udbydere – online markedspladser, søgemaskiner og SoMe

Forskning - forskningsorganisationer

1 **RISIKOVURDERINGER: ALL HAZARD APPROACH**
Alle farer inkl. fysiske

2 **LEVERANDØRSTYRING**
sikkerhe
v
udvil

3 **TEKNIS**
Brug a
autentifil
og
medf



UDDANNELSE AF PERSONALE 4
Personalesikkerhed, grundlæggende cyberhygiejne, politikker og uddannelse

HÅNDTERING AF HÆNDELSER 5
mfatter både

Hvad NIS2 kræver af den direkte omfattede virksomhed
Den NIS2-omfattede virks
- Personalesikkerhed
- **Grundlæggende cyb**
- **Dokumenteret Aware**
- Relevante politikker og p
- Ledelsesansvar for cybe

Det gælder deres egne me
håndtere **risici i forsynings**

Praktisk anbefaling som leverandør
Hvis du leverer til NIS2-omfattede virksomheder, bør du som minimum have:
- **En årlig dokumenteret awareness-træning**
- En informationssikkerhedspolitik
- Rollebaseret træning for tekniske medarbejdere
- En simpel incident-procedure
- Dokumentation klar til kundeaudit

Det behøver ikke være tung ISO-certificering – men det skal være struktureret og dokumenterbart.

Ledelsesforankring og -ansvar

Ledelsen skal:

- Godkende foranstaltninger til styring af Cyber sikkerhed
- Føre tilsyn med implementering i alle enheder
- Gennemføre kurser med henblik på at have tilstrækkelig viden og kompetencer til at styre Cybersikkerheds risici
- Sørge for at der er tilbudt kurser til alle ansatte*
- Tag ansvar for at NIS2-loven overholdes

Kort sagt:
Cybersikkerhed er ikke kun et IT-anliggende – det er et ledelsesansvar. NIS2 forpligter ledelsen til aktivt at sikre de rette kompetencer i organisationen.

*Ifølge § 7, stk. 2 i NIS 2-loven skal ledelsen aktivt tilskynde til, at medarbejdere tilbydes relevante kurser. Ledelsen skal også selv gennemføre relevant uddannelse.

Hvad siger vores kunder

Undersøgelse fra 18. februar

- **ca. 2 ud af 3** arbejder i dag ***ikke*** struktureret og dokumenterbar med awareness-træning.
- **Over halvdelen** peger på *manglende tid, ressourcer eller kompetencer* som den største barriere for at arbejde mere systematisk med IT-sikkerhed.
- **Mange organisationer er enten direkte eller indirekte omfattet af NIS2** – men en betydelig del er stadig i tvivl om deres konkrete rolle og ansvar.
- Mange organisationer er stadig i en **tidlig modenhedsfase.**
- Fokus på IT-sikkerhed drives især af **lovkrav, bestyrelse og reelle hændelser** – ikke af overskud eller god tid.


NIS2

HVAD INDEHOLDER CERTIFICERINGEN?

dansk·it

Reducér menneskelige fejl og dokumentér I lever op til NIS2 awareness træningskravet

NIS2-certificeringen er et introducerende awareness-forløb, der klæder medarbejdere på til at forstå deres rolle i organisationens cybersikkerhed.

Det er ikke et teknisk kursus – Det er et dømmekraftskursus

NIS2 HVORDAN SER DET UD?

Skabt i samarbejde med Dansk IT

En quiz inspireret rejse mod IT-sikkerhed

- En underholdende læringsrejse
- Korte videoer der Fanger modtagerens opmærksomhed
- Baseret på NIS2 kravene til træning
- Øvelser baseret på tvivlssituationer og digitale henvendelser
- Refleksionsopgaver
- Ekspertindslag, der gør stoffet levende og troværdigt

Vært **Mette Valsted**

Tidligere nyhedsvært på DR P1 morgen og TV AVISEN

Kursets opbyning

1. Hvad er NIS2 – og hvorfor er det relevant for dig?
2. NIS2's grundprincipper
3. Hvad betyder cybersikkerhed i din hverdag på jobbet?
4. Genkend risici og trusler
5. Hændelser: Når noget går galt – hvad gør du?
6. NIS2-tjekliste & dit certifikat

Dvs. dækker NIS2 direktivets krav
(Artikel 20(2) – om Awareness og træning)

Målgruppen er “alle”

Men særligt relevant for:

- Administrative funktioner
- Projektledere
- Nye medarbejdere
- Ikke-tekniske teams