unit it

Thomas Boe
Security

NIS2 spøgelset kommer

RED DIG SELV

DATA & CLOUD DAGEN VEST
Aarhus
28. september

NISsen er ikke ny

Målsætningen:

EU's medlemsstater skal vedtage lovgivning af sikkerhedsmæssig karaktér til beskyttelse af 'operatører af væsentlige tjenester' og digitale udbydere.

- NIS i sin nuværende form er vedtaget i EU 19. juli 2016
- Danske NIS vedtaget 4. maj 2018

NIS er et europæisk direktiv, udmøntet i en dansk lov, som efterfølgende har kastet en række bekendtgørelser af sig.

Retsakter

Hvordan er EU's love og regler bliver gældende

Forordning:

Når vi spurgte min mor om vi måtte tage en is og hun svarede: "Nej ikke nu, først når vi har spist…"

Direktiv:

Når vi stillede min far samme spørgsmål og han svarede:

"Jeg synes lige I skal vente lidt"

Retsakter

Hvordan er EU's love og regler bliver gældende

Forordning:

En "forordning" er en bindende retsakt. Det skal følges i alle enkeltheder i alle medlemsstaterne (hele EU)

Direktiv:

En retsakt, der fastsætter et mål, som EU-landene skal opnå. Det er dog op til de enkelte lande at lave deres egne love for, hvordan disse mål skal opnås

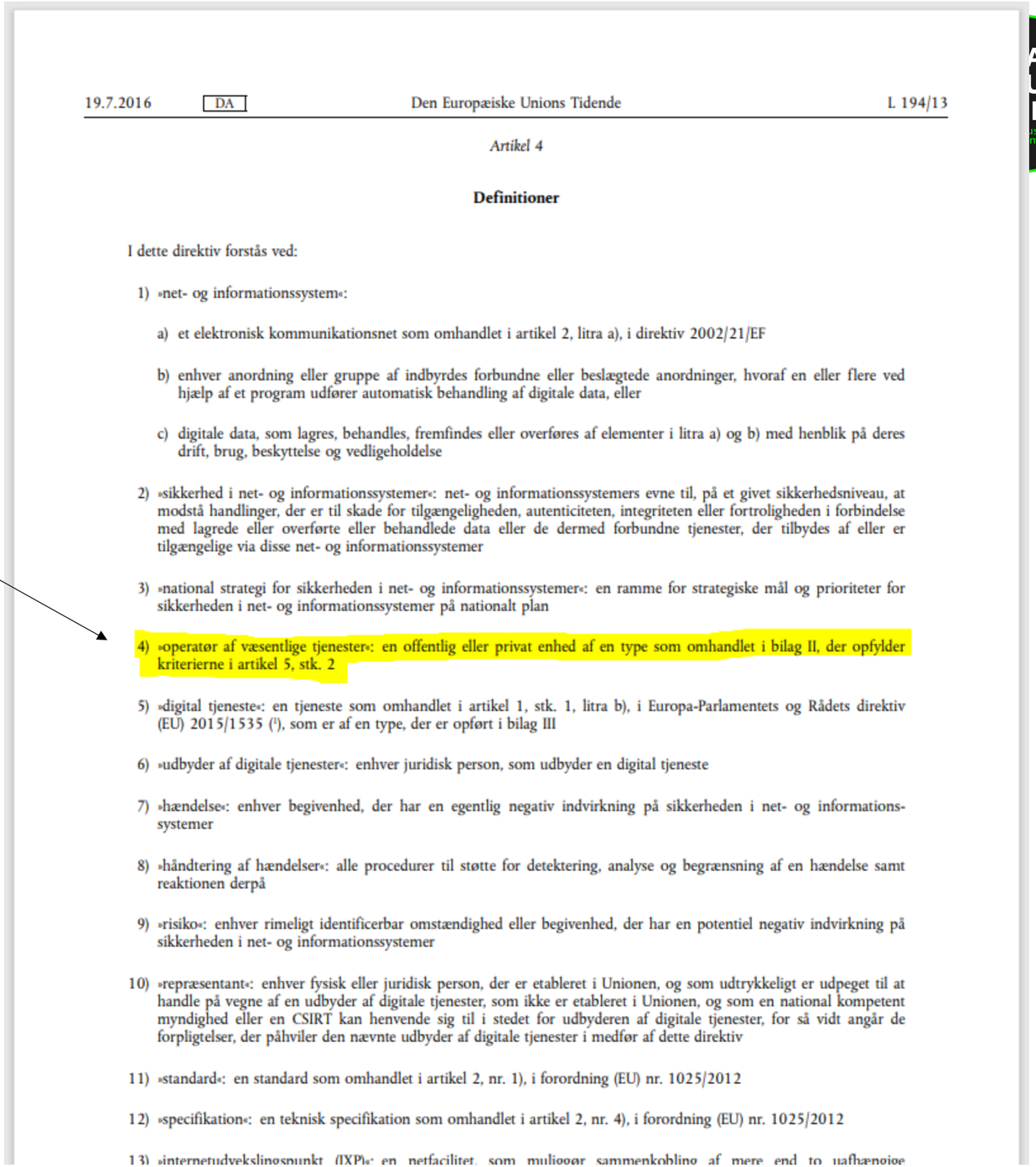
Mest kritisk

Nettjenester og så …..

Artikel 4

Læse læse læse … væsentlige tjenester !!

(Se længere nede)



19.7.2016 DA Den Europæiske Unions Tidende L 194/13

Artikel 4

Definitioner

I dette direktiv forstås ved:

1) »net- og informationssystem«:

a) et elektronisk kommunikationsnet som omhandlet i artikel 2, litra a), i direktiv 2002/21/EF

b) enhver anordning eller gruppe af indbyrdes forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data, eller

c) digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a) og b) med henblik på deres drift, brug, beskyttelse og vedligeholdelse

2) »sikkerhed i net- og informationssystemer«: net- og informationssystemers evne til, på et givet sikkerhedsniveau, at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer

3) »national strategi for sikkerheden i net- og informationssystemer«: en ramme for strategiske mål og prioriteter for sikkerheden i net- og informationssystemer på nationalt plan

4) »operatør af væsentlige tjenester«: en offentlig eller privat enhed af en type som omhandlet i bilag II, der opfylder kriterierne i artikel 5, stk. 2

5) »digital tjeneste«: en tjeneste som omhandlet i artikel 1, stk. 1, litra b), i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 (1), som er af en type, der er opført i bilag III

6) »udbyder af digitale tjenester«: enhver juridisk person, som udbyder en digital tjeneste

7) »hændelse«: enhver begivenhed, der har en egentlig negativ indvirkning på sikkerheden i net- og informationssystemer

8) »håndtering af hændelser«: alle procedurer til støtte for detektering, analyse og begrænsning af en hændelse samt reaktionen derpå

9) »risiko«: enhver rimeligt identificerbar omstændighed eller begivenhed, der har en potentiel negativ indvirkning på sikkerheden i net- og informationssystemer

10) »repræsentant«: enhver fysisk eller juridisk person, der er etableret i Unionen, og som udtrykkeligt er udpeget til at handle på vegne af en udbyder af digitale tjenester, som ikke er etableret i Unionen, og som en national kompetent myndighed eller en CSIRT kan henvende sig til i stedet for udbyderen af digitale tjenester, for så vidt angår de forpligtelser, der påhviler den nævnte udbyder af digitale tjenester i medfør af dette direktiv

11) »standard«: en standard som omhandlet i artikel 2, nr. 1), i forordning (EU) nr. 1025/2012

12) »specifikation«: en teknisk specifikation som omhandlet i artikel 2, nr. 4), i forordning (EU) nr. 1025/2012

13) »internetudvekslingspunkt (IXP)«: en netfacilitet, som muliggør sammenkobling af mere end to uafhængige

Mest kritisk (fortsat)

Nettjenester og så ….

Vi kigger længere nede

Identificering af operatører af væsentlige tjenester…

Se endnu længere nede

Artikel 5

Identificering af operatører af væsentlige tjenester

1. Senest den 9. november 2018 identificerer medlemsstaterne for hver sektor og delsektor, som er omhandlet i bilag II, de operatører af væsentlige tjenester, der er etableret på deres område.

2. De i artikel 4, nr. 4), omhandlede kriterier for identificering af operatører af væsentlige tjenester er følgende:

a) en enhed leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter

b) leveringen af denne tjeneste afhænger af net- og informationssystemer, og

c) en hændelse ville få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste.

3. Med henblik på stk. 1 udarbejder hver medlemsstat en liste over de i stk. 2, litra a), omhandlede tjenester.

4. Med henblik på stk. 1 hører disse medlemsstater hinanden, hvis en enhed leverer en tjeneste, der er omhandlet i stk. 2, litra a), i to eller flere medlemsstater. Denne høring skal finde sted, inden der træffes afgørelse om identificering.

5. Medlemsstaterne tager regelmæssigt og mindst hvert andet år efter den 9. maj 2018 listen over identificerede operatører af væsentlige tjenester op til revision og ajourfører den, hvis det er relevant.

6. Samarbejdsgruppens rolle skal i overensstemmelse med de i artikel 11 omhandlede opgaver være at støtte medlemsstaterne i at anvende en ensartet tilgang, når operatører af væsentlige tjenester identificeres.

7. Med henblik på den i artikel 23 omhandlede revision og senest den 9. november 2018 og herefter hvert andet år forelægger medlemsstaterne Kommissionen de oplysninger, som er nødvendige for, at Kommissionen kan vurdere gennemførelsen af dette direktiv, navnlig ensartetheden i medlemsstaternes fremgangsmåder ved identificeringen af operatører af væsentlige tjenester. Disse oplysninger skal som minimum omfatte:

a) nationale foranstaltninger, som gør det muligt at identificere operatører af væsentlige tjenester

(1) Europa-Parlamentets og Rådets direktiv 2013/11/EU af 21. maj 2013 om alternativ tvistbilæggelse i forbindelse med tvister på forbrugerområdet og om ændring af forordning (EF) nr. 2006/2004 og direktiv 2009/22/EF (direktiv om ATB på forbrugerområdet) (EUT L 165 af 18.6.2013, s. 63).

TYPER AF ENHEDER MED HENBLIK PÅ ARTIKEL 4, NR. 4)

Sektor	Delsektor	Type af enhed
1. Energi	a) Elektricitet	— Elektricitetsvirksomhed som defineret i artikel 2, nr. 35), i Europa-Parlamentets og Rådets direktiv 2009/72/EF (1), der varetager »forsyningen« som defineret i artikel 2, nr. 19), i nævnte direktiv
		— Distributionssystemoperatører som defineret i artikel 2, nr. 6), i direktiv 2009/72/EF
		— Transmissionssystemoperatører som defineret i artikel 2, nr. 4), i direktiv 2009/72/EF
	b) Olie	— Olierørledningsoperatør
		— Operatører af olieproduktion, raffinaderier og behandlingsanlæg, olielagre og olietransmission
	c) Gas	— Forsyningsvirksomheder som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets direktiv 2009/73/EF (2)
		— Distributionssystemoperatører som defineret i artikel 2, nr. 6), i direktiv 2009/73/EF
		— Transmissionssystemoperatører som defineret i artikel 2, nr. 4), i direktiv 2009/73/EF
		— Lagersystemoperatører som defineret i artikel 2, nr. 10), i direktiv 2009/73/EF
		— LNG-systemoperatører som defineret i artikel 2, nr. 12), i direktiv 2009/73/EF
		— Naturgasvirksomheder som defineret i artikel 2, nr. 1), i direktiv 2009/73/EF
		— Naturgasoperatør, raffinaderier og behandlingsanlæg
2. Transport	a) Lufttransport	— Luftfartsselskaber som defineret i artikel 3, nr. 4), i Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 (3)
		— Lufthavnsdriftsorganer som defineret i artikel 2, nr. 2), i Europa-Parlamentets og Rådets direktiv 2009/12/EF (4), lufthavne som defineret i artikel 2, nr. 1), i nævnte direktiv, herunder de hovedlufthavne, der er anført i afsnit 2 i bilag II til Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013 (5); og enheder med tilknyttede anlæg i lufthavne
		— Trafikledelses- og kontroloperatører, der udøver flyvekontroltjeneste som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004 (6)
	b) Jernbanetransport	— Infrastrukturforvalter som defineret i artikel 3, nr. 2), i Europa-Parlamentets og Rådets direktiv 2012/34/EU (7)
		— som defineret i artikel 3, nr. 1), i direktiv 2012/34/EU, herunder operatører af servicefaciliteter som defineret i artikel 3, nr. 12), i direktiv 2012/34/EU
	c) Søfart	— Rederier, som udfører passager- og godstransport ad indre vandveje, i højsøfarvand eller kystnært farvand som defineret for søtransport i bilag I til Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004 (8), bortset fra de enkelte fartøjer, som drives af disse rederier
		— Havnedriftsorganer som defineret i artikel 3, nr. 1), i Europa-Parlamentets og Rådets direktiv 2005/65/EF (9), herunder deres havnefaciliteter som defineret i artikel 2, nr. 11), i forordning (EF) nr. 725/2004 (8), i forbindelse med aktiviteter styr i havne
		— Skibstrafiktjenesteoperatø i Europa-Parlamentets og
	d) Vejtransport	— Vejmyndigheder som defi nens delegerede forordni svarlige for trafikledelse
		— Operatører af intelligente transportsystemer som defineret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets direktiv 2010/40/EU (12)
3. Bankvæsen		Kreditinstitutter som defineret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 (13)
4. Finansielle markedsinfrastrukturer		— Markedspladsoperatører som defineret i artikel 4, nr. 24), i Europa-Parlamentets og Rådets direktiv 2014/65/EU (14)
		— Central modpart (CCP) som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 (15)
5. Sundhedssektoren	Sundhedstjenestemiljøer (herunder hospitaler og private klinikker)	Sundhedstjenesteydere som defineret i artikel 3, litra g), i Europa-Parlamentets og Rådets direktiv 2011/24/EU (16)
6. Drikkevandsforsyning og distribution		Leverandør og distributør af »drikkevand« som defineret i artikel 2, nr. 1), litra a), i Rådets direktiv 98/83/EF (17) bortset fra distributører, for hvem distribution af drikkevand kun er en del af deres generelle aktivitet med distribution af andre råvarer og varer, der ikke anses som væsentlige tjenester.
7. Digital infrastruktur		— IXP'er
		— DNS-tjenesteudbyder
		— TLD-navneadministratorer

Kritisk vand

Bekendtgørelse: Vand er kritisk

Minister udtaler:

"Vand skal have cybersikkerhed, vi vurderer p.t. sammen med regeringens støttepartier at indkøbe flydende antivirusbeskyttelse som kan tilsættes drikkevandsboringer i tætbefolkede områder"

Professor Emeritus Jørgen Svovlpøl
DTU

"Jeg har aldrig hørt noget lignende"

Ekstra Bladet

Køb abonnement

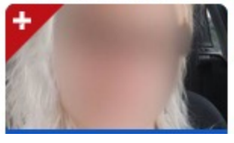
Vand er blevet kritisk

Drikker ikke VAND

LIVE

Brøndby dropper vandet

Mere fra Ekstra Bladet+



https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A829%3AFIN

zero 0/0

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I
SUBJECT MATTER , SCOPE AND DEFINITIONS

Article 1
Subject matter and scope

1. This Directive:

(a) lays down obligations for Member States to take certain measures aimed at ensuring the provision in the internal market of services essential for the maintenance of vital societal functions or economic activities, in particular to identify critical entities and entities to be treated as equivalent in certain respects, and to enable them to meet their obligations;

(b) establishes obligations for critical entities aimed at enhancing their resilience and improving their ability to provide those services in the internal market;

(c) establishes rules on supervision and enforcement of critical entities, and specific oversight of critical entities considered to be of particular European significance.

2. This Directive shall not apply to matters covered by Directive (EU) XX/YY [proposed Directive on measures for a high common level of cybersecurity across the Union; ('NIS 2 Directive')], without prejudice to Article 7.

3. Where provisions of sector-specific acts of Union law require critical entities to take measures as set out in Chapter III, and where those requirements are at least equivalent to the obligations laid down in this Directive, the relevant provisions of this Directive shall not apply, including the provisions on supervision and enforcement laid down in Chapter VI.

4. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of critical entities.

mest pressererende spørgsm
zero trust.

Har du brug for at få et overblik over din virksomheds IT-sikkerhed? Så kontakt os endelig på [redacted] eller på [redacted].

og forskning.

DATA & CLOUD DAGEN WEST
Aarhus
28. september

Kritisk vand

Bekendtgørelse: Vand er kritisk

GÆLDENDE

BEK nr 429 af 04/05/2018 Miljøministeriet

NIS-bekendtgørelsen Yderligere oplysninger >

Bekendtgørelse om krav til sikkerheden i visse vandforsyningers net- og

ng m.v., jf. lovbekendtgørelse nr. 118

1, og fastsætter regler om de

kerheden i de net- og

pningen.

eden i net- og informationssystemer.

2) Håndtering af hændelser: Alle procedurer til støtte for detektering, analyse og begrænsning af en hændelse samt reaktionen derpå.

3) Net- og informationssystem:

a) et elektronisk kommunikationsnet som omhandlet i artikel 2, litra a), i direktiv 2002/21/EF,

b) enhver anordning eller gruppe af indbyrdes forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data, eller

c) digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a) og b) med henblik på deres drift, brug, beskyttelse og vedligeholdelse.

4) Operatør af væsentlige tjenester af vandforsyning og -distribution: Vandforsyninger, som fremgår af bilag 2, punkt 6, i Europa-Parlamentets og Rådets direktiv (EU) 2016/1148, og som opfylder kriterierne i direktivets artikel 5, stk. 2.

5) Risiko: Enhver rimeligt identificerbar omstændighed eller begivenhed, der har en potentiel negativ indvirkning på

Bilag 1

Oversigt overoperatører af væsentlige tjenester af vandforsyning og –distribution, jf. § 3

Ingen vandforsyninger.

Officielle noter

Opsummering

Væsentlige tjenester – leverer kritiske samfundsmæssige eller økonomiske aktiviteter

Ét begreb = Væsentlig, defineres i artikel 5

Omfatter følgende områder

Energi: Elektricitet, Olie, Gas

Transport: Luft, jernbane, sø, vej (trafikledelse)

Bank: Kreditinstritutter

Finansielle markedsinfrastrukturer:

Sundhedssektoren: Hospitaler, private klinikker

Drikkevandsforsyning: Leverandør og distributør

Digital infrastruktur: DNS udbydere, IXP, TopLevel

Faktaboks

I kommende NIS2 arbejdes med 2 begreber

- Væsentlige
- Vigtige

Kritisk EL og Naturgas

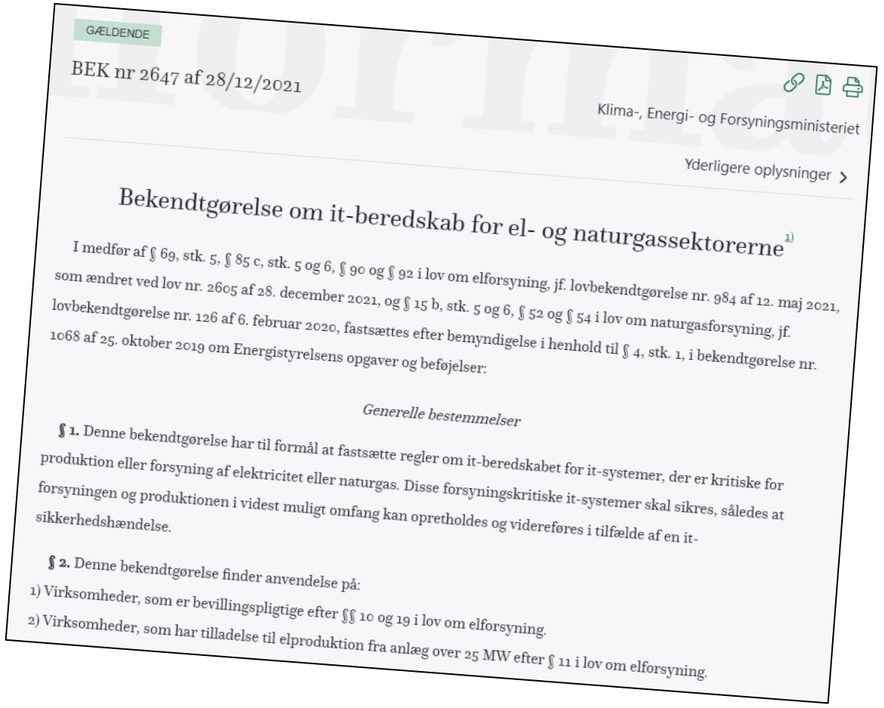
Bekendtgørelse om IT beredskab

Bekendtgørelse 2647 (tidl 820, tidl 425 tidl 515)

- Kategorisering (stor større størst)
- Organisering (roller og ansvar – beredskab only)
- Risiko og sårbarhedsvurderinger
- Identificere kritiske systemer
- Udarbejde og øve beredskabsmaterialer
- Beskytte kritiske IT systemer
- Levarandørstyring
- IT sikkerhedstjeneste
- Der laves (årlige) tilsyn

Faktaboks

Ordet "cyber" indgår 4 gange i bekendtgørelsen…



GÆLDENDE

BEK nr 2647 af 28/12/2021

Klima-, Energi- og Forsyningsministeriet

Yderligere oplysninger

Bekendtgørelse om it-beredskab for el- og naturgassektorerne[1)]

I medfør af § 69, stk. 5, § 85 c, stk. 5 og 6, § 90 og § 92 i lov om elforsyning, jf. lovbekendtgørelse nr. 984 af 12. maj 2021, som ændret ved lov nr. 2605 af 28. december 2021, og § 15 b, stk. 5 og 6, § 52 og § 54 i lov om naturgasforsyning, jf. lovbekendtgørelse nr. 126 af 6. februar 2020, fastsættes efter bemyndigelse i henhold til § 4, stk. 1, i bekendtgørelse nr. 1068 af 25. oktober 2019 om Energistyrelsens opgaver og beføjelser:

Generelle bestemmelser

§ 1. Denne bekendtgørelse har til formål at fastsætte regler om it-beredskabet for it-systemer, der er kritiske for produktion eller forsyning af elektricitet eller naturgas. Disse forsyningskritiske it-systemer skal sikres, således at forsyningen og produktionen i videst muligt omfang kan opretholdes og videreføres i tilfælde af en it-sikkerhedshændelse.

§ 2. Denne bekendtgørelse finder anvendelse på:

1) Virksomheder, som er bevillingspligtige efter §§ 10 og 19 i lov om elforsyning.

2) Virksomheder, som har tilladelse til elproduktion fra anlæg over 25 MW efter § 11 i lov om elforsyning.

Tilføjelse NIS2

I overskriftsform hvad er så nyt

NIS2: *Væsentlige enheder er:*

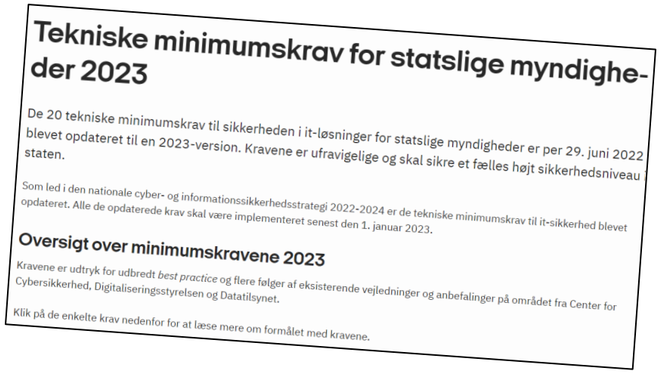
- **Energi** (*Fjernvarme, brint, producenter*)
- Transport
- Bankvæsen
- finansielle markedsinfrastrukturer
- Sundhed
- Drikkevand
- **Spildevand**
- Digital infrastruktur
- Offentlig forvaltning
- **Rummet**

NIS2: *Vigtige enheder er:*

- **Post- og kurertjenester**
- **Affaldshåndteringfremstilling**
- **Fremstilling og distribution af kemikalier**
- **Fødevareproduktion, -forarbejdning og -distribution**
- **Fremstillingsvirksomhed**
- Digitale udbydere

Cyber vs. Cyber ikke

Velmenende forslag til cybersikkerhed



Tekniske minimumskrav for statslige myndighe-der 2023

De 20 tekniske minimumskrav til sikkerheden i it-løsninger for statslige myndigheder er per 29. juni 2022 blevet opdateret til en 2023-version. Kravene er ufravigelige og skal sikre et fælles højt sikkerhedsniveau staten.

Som led i den nationale cyber- og informationssikkerhedsstrategi 2022-2024 er de tekniske minimumskrav til it-sikkerhed blevet opdateret. Alle de opdaterede krav skal være implementeret senest den 1. januar 2023.

Oversigt over minimumskravene 2023

Kravene er udtryk for udbredt *best practice* og flere følger af eksisterende vejledninger og anbefalinger på området fra Center for Cybersikkerhed, Digitaliseringsstyrelsen og Datatilsynet.

Klik på de enkelte krav nedenfor for at læse mere om formålet med kravene.

Slutproduktet handler om at være i kontrol.

- Er vores kritiske processer identificerede?
- Er vi i kontrol med de data (systemer og komponenter) som processerne er afhængige af?
- Hvilke risici er der for at vi ikke længere er i kontrol?
- Hvad gør vi hvis vi mister kontrollen?
  - Ansvar (kommunikation)
  - Planer (beredskab)

Nogle forslag til bedre cybersikkerhed er:

- Firewall på alle klienter
- Harddiske skal krypteres
- Emails skal være krypterede
- Telefoner skal have adgangskode
- Netværk skal anvende sikker DNS
- Wifi netværk skal krypteres

Alle sammen gode velmenende forslag til ”IT sikkerheden for statslige myndigheder”

MEN

Cyber vs. Cyber ikke

Velmenende forslag til cybersikkerhed

Cyber vs. Cyber ikke

Velmenende forslag til cybersikkerhed

Brødbanditterne A/S

Slutproduktet handler om at være i kontrol.

- Er vores kritiske processer identificerede?
- Er vi i kontrol med de data (systemer og komponenter) som processerne er afhængige af?
- Hvilke risici er der for at vi ikke længere er i kontrol?
- Hvad gør vi hvis vi mister kontrollen?
  - Ansvar (kommunikation)
  - Planer (beredskab)

Cyber vs. Cyber ikke

Velmenende forslag til cybersikkerhed

Slutproduktet handler om at være i kontrol.

- Er vores kritiske processer identificerede?
- Er vi i kontrol med de data (systemer og komponenter) som processerne er afhængige af?
- Hvilke risici er der for at vi ikke længere er i kontrol?
- Hvad gør vi hvis vi mister kontrollen?
  - Ansvar (kommunikation)
  - Planer (beredskab)

Brødbanditterne A/S

PLC'er – Industrial control systems

- Intet WIFI
- Ingen mail
- Ingen harddisk der kan krypteres
- Andre netværksprotokoller ikke egnet til kryptering eller værste fald umulige af kryptere

NIS2 brudt ned

Slutproduktet er styrkelse af cyber, og skal opnås gennem compliance

Den enkelte stat skal: 5-11

- Udarbejde en strategi med mål og foranstaltninger
- Udpege kompetente myndigheder

Alle stater skal: 12-16

- Fælles EU netværk CyCLONe netværk sikk. Org.
- Peer review af andres politikker

Risikostyring: 17-23

- Passende tekniske og org. Foranstaltninger* PTOF
- Direktionen er ansvarlig og trænes risikostyring
- EU kan tvinge medlemsstaterne til PTOF

HVAD?
Ingen nye bitlocker, firewalls, VPN, Endpoint, 802.1x, TLS, dytbåt dynamolygte??

NIS2 brudt ned

Vi ved allerede hvilke 7 områder der vil blive udmøntet

***Passende tekniske og org. Foranstaltninger* PTOF**

- Politik for risikoanalyse og informationssikkerhed
- Håndtering af hændelser
- Krisestyring
- Forsyningskædesikkerhed
- Sikkerhed ved indkøb og udvikling og håndtering/offentliggørelse af sårbarheder
- Interne kontroller til vurdering af alt ovenstående
- Brug af kryptering

EU kommissionen peger altså på at der er 7 fundamentale discipliner som bliver vigtige at have på plads når de danske bekendtgørelser rammer på direktionsgangene.

Bare husk på de 7 små dværge

NIS2 brudt ned

Nu bliver det for alvor spændende

Den enkelte stat skal: 5-11

- Udarbejde en strategi med mål og foranstaltninger
- Udpege kompetente myndigheder

Alle stater skal: 12-16

- Fælles EU netværk CyCLONe netværk sikk. Org.
- Peer review af andres politikker

Risikostyring: 17-23

- Passende tekniske og org. Foranstaltninger* PTOF
- Direktionen er ansvarlig og trænes risikostyring
- EU kan tvinge medlemsstaterne til PTOF

Standardisering: 22

- Der tilskyndes (juridisk sprog for at man BØR) certificeres.

Det skal være en Europæisk eller international standard som er relevant for "informationssystemer".

Hvad nu hvis: 24

- En aktør har hjemmehørende udenfor EU

Aktører som dette gælder for: 25

Rumfart, el, vand osv. Osv.

Print table Download as .XLS

1. Main View

2. Filters Security domain Security measure Standards Apply Filters

SECURITY MEASURES	STANDARDS		
	ISO 27001	NIST CSF	ISA/IEC 62443
Incident Report	▪ 7.5 Documented information ▪ A.12.1.1 Documented operating procedures ▪ A.16.1.1 Responsibilities and procedures ▪ A.16.1.2 Reporting information security events ▪ A.16.1.3 Reporting information security weaknesses	▪ RS.CO - 2, 3, 4, 5 ▪ DE.DP-4	▪ SR 2.8 ▪ SR 2.9 ▪ SR 2.10 ▪ SR 2.11 ▪ SR 2.12 ▪ SR 3.9 ▪ SR 6.1 ▪ SR 6.2
Communication with competent authorities	▪ 7.4 Communication ▪ 7.5 Documented information ▪ A.6.1.3 Contact with authorities	▪ RS.CO - 2, 3, 4, 5 ▪ DE.DP-4	▪ SR 2.8 ▪ SR 2.9 ▪ SR 2.10

Opsummering

Medlemsstaterne sikrer, at overtrædelser af forpligtelserne i artikel 18 eller artikel 20 i overensstemmelse med nærværende artikels stk. 2 og 3 straffes med administrative bøder på maksimalt mindst 10 000 000 EUR eller op til 2 % af den samlede globale årsomsætning i den virksomhed, som den væsentlige eller vigtige enhed tilhører i det foregående regnskabsår, alt efter hvad der er højest.

1. Flere aktører medtages
2. Der etableres flere tilsynsmyndigheder
3. Samarbejde mellem staterne
4. Ingen lande slipper med "løs" lovgivning
5. Aktører skal håndtere "de 7 små dværge"
6. Direktionen er direkte ansvarlig
7. Aktører kan/skal/bør certificeres

8. Kontrol
9. Bødestørrelser

WE MADE IT!!!

Er I fortsat vågne?

Spørgsmål

NIS2 har et klart formål. (egen simplificering)

At kvalificere virksomhederne til at styre risici.

At øge samarbejdet* på tværs i Europa.

*kontrol, viden, notificering