Bliv klar til NIS2-direktivet for den offentlige sektor

Beredskabsplanlægning i praksis

Webinar, torsdag den 3. juni 2021

pwc

Revision. Skat. Rådgivning.

CENTER FOR CYBERSIKKERHED

Revision af NIS-direktivet

Policychef Eva Leisner, Center for Cybersikkerhed

3. juni 2021

Dagsorden

- Formål og opbygning
- Hvor er vi i dag?
- Udkast til NIS2:

- *National strategi, krisestyringsplan, kontaktpunkt og CSIRT*
- *Udvidelse af dækningsområdet*
- *Krav til kompetente myndigheder og udbydere*
- *Underretning om hændelser*
- *Dansk holdning og forhandlingssituationen*

Formålet

Fortsat at sikre et højt cybersikkerhedsniveau i EU gennem

- nationale strategier mv.
- krav om risikostyring, passende sikkerhedstiltag og underretning fra en væsentligt udvidet kreds af udbydere samt
- forpligtelse til videndeling

Altså

1. Læg en plan!
2. Få styr på, hvad I har, og opdag, når der sker noget!
3. Fortæl om det!

Opbygningen – digitale afhængigheder

Hvor er vi i dag?

- **6+1 sektorer:** Energi (el, olie, gas), transport (luft, bane, sø, vej), bank, finansmarkeder, sundhed, drikkevand, digital infrastruktur og digitale tjenester (ikke tele)
- **Udpegning af væsentlige operatører (OES'er):** Myndighederne har identificeret de udbydere af tjenester som omfattes af direktivets krav. (+ DSP implementeringsforordning)
- Krav om **underretning om væsentlige hændelser** til kompetent myndighed og CSIRT. Sker via *virk.dk*. Orientere om grænseoverskridende hændelser til EU-medlemslande og årlig indberetning til ENISA
- **Sektorbaseret** implementering i dansk sammenhæng

NIS2: Nationalt niveau

- National strategi med mål, prioriteter og governancestruktur (art. 5)
- Identifikation af beredskabs- og genopretningsforanstaltninger
- Vedtage en række politikker som led i strategien, herunder CVD, forsyningskæder og tilgængelighed af internettet
- Evalueres mindst hvert 4. år
- Krisestyringsplan (art. 7)
- Nationalt kontaktpunkt og CSIRT (art. 8 og 9)

Nationale rammer for styring af cybersikkerhedskriser (art. 7)

Hver medlemsstat vedtager en national cybersikkerhedshændelses- og kriseberedskabsplan, der navnlig skal indeholde følgende:

- målsætninger for nationale beredskabsforanstaltninger og -aktiviteter
- de nationale kompetente myndigheders opgaver og ansvarsområder
- krisestyringsprocedurer og informationsudvekslingskanaler
- beredskabsforanstaltninger, herunder øvelses- og uddannelsesaktiviteter
- relevante berørte offentlige og private interesserede parter og infrastruktur
- nationale procedurer og ordninger for at sikre effektiv deltagelse i håndteringen af væsentlige hændelser og kriser på EU-plan

Udvidelse af dækningsområdet

Væsentlige enheder

Listen over væsentlige enheder svarer til det gældende NIS-direktiv, dog udvidet på energiområdet (fjernvarme, el-marked, olielagre, brint) samt med spildevand, offentlig administration (centraladministration og regioner) og jordbaseret infrastruktur vedrørende rumfart.
Afgrænsningen af digital infrastruktur er udvidet betydeligt med cloud computing, datacentre, CDN (indholdsdistribution), trust-udbydere samt teletjenester.

Vigtige enheder

Listen over vigtige enheder omfatter post og udbringning, affaldshåndtering, kemiske produkter (fremstilling og distribution), fødevarer (fremstilling og distribution), fremstilling på visse områder (pharma, computer/elektronik og optisk udstyr, elektrisk udstyr, maskineri, køretøjer samt andet transportudstyr), samt digitale udbydere (online markedspladser, søgemaskiner og sociale platforme).

NIS2: Nye krav til udbydere og nye pligter for myndighederne

- Ny skelnen ml. hhv. **væsentlige** og **vigtige** sektorer, alle udbydere af tjenester inden for dækningsområdet omfattes af direktivets krav, undtagen mikrovirksomheder. Dvs. ingen udpegning af OES'er.

- **Krav til udbyderne** om risikostyring og sikkerhedstiltag (bl.a. bestyrelsesansvar, hændelseshåndtering, business continuity, leverandørstyring og kryptering) (art. 18)

- **Pligt for kompetente myndigheder** om aktivt tilsyn og væsentlig udvidet underretningsforpligtelse til ENISA (månedligt) (bl.a. art. 29 og 30)

Kompetente myndigheder - risikobaseret tilsyn

Art. 29 og 30 angiver omfanget af de kompetente myndigheders tilsyn, *som skal være risikobaseret* – herunder hjemmel til (jf. art. 18):

- kontrol on-site, revisioner og sikkerhedsscanninger
- anmodning om oplysninger og data for at vurdere sikkerhedsforanstaltninger, herunder dokumenterede politikker
- udstedelse af pålæg om mitigerende tiltag og/eller underretning af berørt 3. part
- pålægge enheder at offentliggøre aspekter af manglende overholdelse af regler, herunder offentligt identificere ansvarlige personer
- udstede bødeforlæg (størrelser svarer til GDPR)

Underretning om hændelser

- Enheder underrette om væsentlige hændelser og særlige observerede trusler (”nærvedhændelser”)
- Udvidelsen af dækningsområdet vil betyde vækst i mængden af underretninger = mere viden om sårbarheder
- CSIRT varsler andre lande hvor relevant pba. underretninger
- Kompetente myndigheder i dialog med underretter hvor relevant.
- Nationalt kontaktpunkt skal indberette månedligt til ENISA om antal og art af underretninger.

Oversigt

	Nationale Strategier	Kontaktpunkt og CSIRT = CFCS	Kompetente myndigheder	Udbydere/enheder
Nyt NIS2	Mål, prioriteter og governance. Identifikation af beredskabs og genopretningsforanstalt-ninger (ny) Vedtage en række cyberpolitikker som led i strategien, herunder CVD, forsyningskæder og tilgængelighed af internettet (ny) Evalueres mindst hvert 4. år (ny) Krisestyringsplan (ny)	Indsende hændelsesrapporter til ENISA månedligt (ny) Samarbejde med sektorfællesskaber (ny) Deltage i peerevalueringer (ny) Monitorere cybertrusler, -sårbarheder og -hændelser Levere tidlig varsling Foretage proaktiv sikkerhedsskanning på anmodning fra enheder (ny) Rådgive enheder om afbødende foranstaltninger ved hændelser (ny)	Udvides med flere sektorer, der omfatter væsentlige og vigtige enheder (ny) Føre tilsyn med væsentlige enheder og håndhæve sikkerhedsbrud (ny) Føre ex post tilsyn med vigtige enheder og håndhæve sikkerhedsbrud (ny) Udstede advarsler og mulighed for pålægge enheder at udbedre sikkerhedsmangler (ny) Samarbejde med kompetente myndigheder udpeget jf. direktivet om kritiske enheders modstandsdygtighed (ny) Tilskynde brug af anerkendte sikkerheds-standarder i enhederne (ny)	Udvides med væsentlige og vigtige enheder i sektorer (ny) Ledelsen skal involveres i styring af cybersikkerhedsrisici (ny) Træffe en række skærpede sikkerhedsforanstaltninger, herunder risikovurdering, hændelseshåndtering, krisestyring, kryptering, forsyningskædesikkerhed samt sikkerhedsskanninger ifbm. tilsyn. Underrette CSIRT eller den kompetente myndighed max. 24 timer efter kendskab til sikkerhedshændelse (ny) Tage hensyn til sårbarheder ved leverandører (ny) Korrigere sikkerhedsforanstaltninger, hvis de ikke lever op til krav Underrette CSIRT eller kompetent myndighed om alle cybertrusler, der kunne resultere i en hændelse (ny)

National holdning til NIS2

Grund- og nærhedsnotat til Folketingets Europaudvalg

Forslaget flugter i høj grad med regeringens syn på beskyttelse af kritisk infrastruktur. Regeringen støtter fokus på øget samarbejde og vidensdeling.

Vigtigt, at NIS-direktivet ikke medfører uforholdsmæssige eller unødige økonomiske byrder for aktører, der ikke er samfundsmæssigt eller økonomisk vigtige + at der tages hensyn til allerede eksisterende regulering og krav i sektorerne.

Vigtigt, at Danmark kan implementere efter sektoransvarsprincippet.

Udvidelse af NIS-direktivets dækningsområde i bredden og dybden skal ske med udgangspunkt i en risikobaseret tilgang. Regeringen vil arbejde for at begrænse unødige administrative byrder.

Forhandlingen af NIS2

Behandling i rådsarbejdsgruppen

- Forhandlinger af KOM's forslag ventes at pågå året ud -> fransk formandskab i 1. halvår 2022
- Implementering i dansk ret inden 18 måneder efter direktivets ikrafttræden. Dvs. udformning af nationale regler i 2022-2023? Ikrafttræden i 2023?
- Forudsat i dansk holdning at implementering skal kunne ske sektorvis, og at sektormyndigheder ligesom i dag vil være kompetente NIS-myndigheder
- Særligt opmærksomhedspunkt på at implementering ikke medfører uhensigtsmæssige konflikter for aktører, som opererer i flere sektorer.

Spørgsmål?

sikker digital DK

@cybersikkerhed
@CFCSsitcen

www.cfcs.dk
www.sikkerdigital.dk

Bliv klar til NIS2-direktivet for den offentlige sektor

Beredskabsplanlægning i praksis

Webinar, torsdag den 3. juni 2021

pwc

Revision. Skat. Rådgivning.

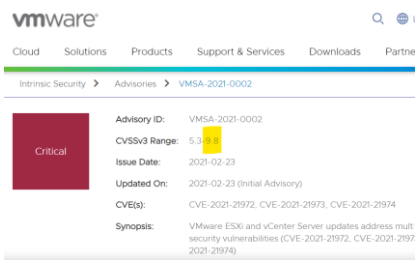
Hvad er problemet?

Sikkerhedshændelser vil opstå

Cyber incidents

2021 Cyber-gyserhistore på seks ord:

“SolarWinds og Exchange OWA på Vmware”



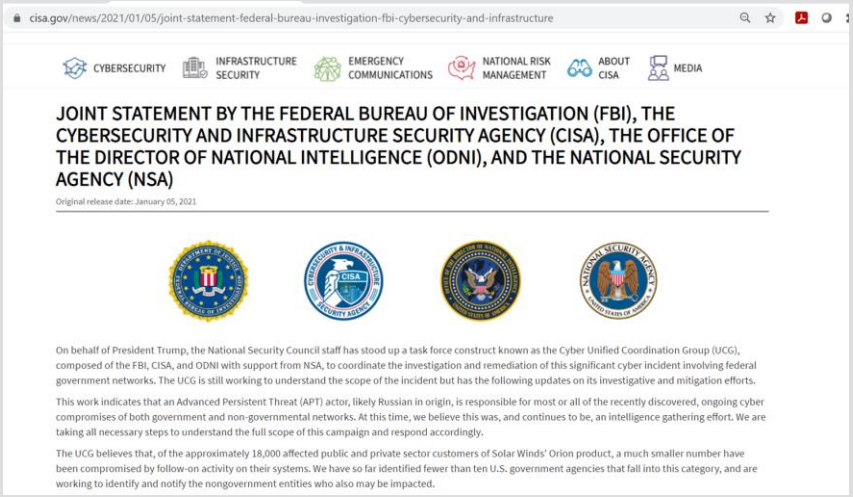
Kilder: SolarWinds (russisk angreb): https://cfcs.dk/da/handelser/varsler/varsel-om-solarwinds-kompromittering/
Exchange (Kinesisk angreb som derefter blev udnyttet af cyberkriminelle) https://cfcs.dk/da/nyheder/2021/cfcs-advarer-om-exchange-sarbarheder/
Vmware: https://www.vmware.com/security/advisories/VMSA-2021-0002.html

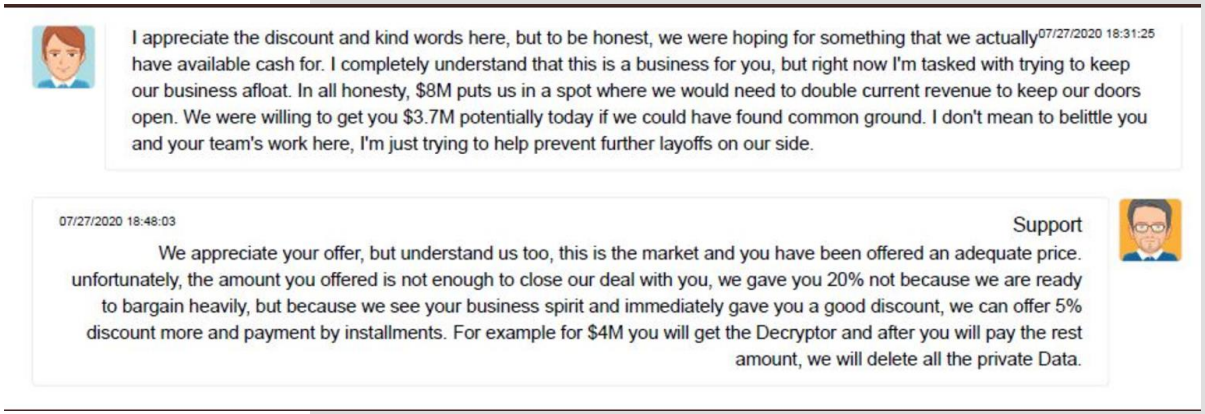
Ufuldstændig sikring

Hvem udgør problemet?

1. **Stater og statssponsorerede aktører**
2. **Cyberkriminelle**
3. **Cyberaktivister**
4. **Cyberterrorister**

PwC's Cyber Crime Survey 2020
79 % af respondenterne har været udsat for phishingangreb. Læs mere på: www.pwc.dk/cybersurvey





Kilde: https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

Hvad kan man gøre ved det?

Readiness is all

1

Kend din organisations kapacitet og kapabilitet inden for beredskab, og afstem forventninger til reetablering med forretningen.

2

Etablér en operationel krisestyringsorganisation og -plan.

3

Få etableret forudsætningerne for forretningskontinuitet.

4

Træn din egen organisation i krisestyring og beredskab, herunder disaster recovery.

Hvad skal man kunne som organisation for at kriselede?

Hvad kræves af en operationel plan?

Kriseledelse består af fire elementer

1

Aktivering og drift af kriseorganisationen.

2

Styring af information.

3

Koordination af ressourcer og handlinger.

4

Kommunikation.

Gør planen overskuelig i en krise

Skriv principperne i planen

Brug action cards til at beskrive handlinger, der skal udføres

Action card no. x: agenda of the first meeting of the crisis management team

Task Action card no. 2 is activated when Crisis Management is activated
Manager Crisis Manager
Organisation CMT is mobilized physically or online
Staffing Necessary CMT members
Content of the Agenda 1. Participants and Scribe (taker of minutes and logging) 2. Appointment of crisis manager, roles and responsibilities, in particular the Communication manager 3. The situation: Incident Management describes situation from Situational overview: template. 4. Crisis Manager formulates mission objective 5. Determination of organization (daily organization, staff activation or full operation) 6. Staffing (redundancies and redistribution) 7. Identification of relevant **stakeholders** • Who is impacted? • Does CFCS-DK need information or activation? 8. **Legal and regulatory stream**. Contact legal Department • Is it a data breach and potential GDPR incident? 9. **Communication** (external and internal) • Decide communication strategy. • Prepare communications to internal Ramboll staff 10. Activation experience 11. Any Other Business 12. Summary of significant decisions

Hvordan griber PwC typisk en beredskabsopgave an?

Sikr at plan, organisation, kapacitet og kapabilitet er afstemt

1

Da reetablering efter en sikkerhedshændelse typisk er en it-tung opgave, begynder PwC med at vurdere it-organisationens (intern eller outsourcet) kapacitet og kapabilitet ved at gennemføre tre scenariedrevne workshops eller øvelser, hvor vi afklarer den faktiske beredskabsevne herunder disaster recovery.

2

To af øvelserne går på trusselsbaserede scenarie mod organisationen, fx truslen fra cyberkriminelle via ransomware. De fire elementer i kriseledelse afprøves ved samme lejlighed.

3

På baggrund af de to øvelser, udarbejder PwC et antal observationer for organisations tekniske beredskabsevner, herunder en vurdering af den faktiske reetableringstid og -effektivitet. Observationer afstemmes med it-organisationen.

4

Sammen med forretningen gennemfører PwC de services/it-systemer/processer, som er nødvendige for forretningskontinuitet og afstemmer forretningens krav til reetablering ift. it-organisationens kapacitet og kapabilitet. Herunder afklares også, om der i organisationen er en organisation til kriseledelse.

5

PwC udarbejder sammen med forretningen og it-organisationen en vurdering af organisationens faktiske beredskabsevne med tilhørende anbefalinger.

Træn din organisation

1

Enhver plan er kun papir, hvis den ikke øves.

2

Brug planlagte reetableringstests i it-organisationen eller mindre it-hændelser til at træne kriseledelsen.

3

Sørg for at træne alle i organisationen, som forventes at have en rolle at spille under en krise.

Kontakt os gerne for spørgsmål

Thomas Kristmar
PwC | Director, Cyber Security
M: +45 5087 9661
E: thomas.kristmar@pwc.com

Succes skaber vi sammen …

www.pwc.dk