NIS 2

VEJLEDNING TIL NIS 2-LOVEN

IMPLEMENTERING AF CYBERSIKKERHEDS-FORANSTALTNINGER

Denne vejledning skal hjælpe offentlige og private enheder med at implementere de foranstaltninger til styring af cybersikkerhedsrisici, der er i NIS 2-loven

Styrelsen for Samfundssikkerhed

NIS 2-VEJLEDNING

Denne vejledning er udarbejdet af Styrelsen for Samfundssikkerhed. Vejledningen er generel og henvender sig til enheder i alle sektorer, der er omfattet af NIS 2-loven. Den kan suppleres af mere sektorspecifik vejledning ved den relevante sektoransvarlige myndighed. Det er i alle tilfælde den relevante sektoransvarlige myndighed, der vurderer, om en enhed lever op til forpligtigelserne i NIS 2-loven.

Datavej 20
3460 Birkerød
Telefon: +45 4516 1666
Mail: nis2@samsik.dk

1. udgave juni 2025.

Styrelsen for Samfundssikkerhed

INDHOLD

ORDLISTE

AKTIV
En identificerbar komponent – fysisk, digital eller organisatorisk – der understøtter funktionaliteten, sikkerheden eller tilgængeligheden af net- og informationssystemer, og som har betydning for leveringen af væsentlige eller vigtige tjenester. Dette kan inkludere hardware, software, data, netværk, processer og personale, eller andet som har værdi for enheden.

AUTENTICITET
Autencitet betyder, at en person eller et system er, hvad den eller det forgiver at være.

CSIRT (COMPUTER SECURITY INCIDENT RESPONSE TEAM)
En national eller sektorbaseret enhed, udpeget eller oprettet af en medlemsstat i EU i henhold til artikel 10 i NIS2-direktivet, med ansvar for at forebygge, detektere og håndtere cybersikkerheds-hændelser. I Danmark er CSIRT'en en national enhed. CSIRT'ens opgaver omfatter bl.a. hændelses-håndtering, varsling og koordinering med relevante myndigheder og private aktører. CSIRT'en er en central aktør i både den nationale cybersikkerhedsstruktur og i det europæiske CSIRT-netværk, jf. artikel 15 i NIS 2-direktivet, med fokus på samarbejde og informationsdeling på tværs af medlemsstaterne.

CYBERHYGIEJNE
Cyberhygiejne dækker over de grundlæggende foranstaltninger og daglige sikkerhedsvaner, praksisser og procedurer, som beskytter netværk, systemer og data mod almindelige trusler. Det omfatter f.eks. brug af stærke passwords, regelmæssig opdatering af software, sikkerhedskopiering, brug af antivirus samt opmærksomhed på phishing og andre digitale angreb.

CYBERSIKKERHED
De aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, brugerne af sådanne systemer og andre personer berørt af cybertrusler.

DIREKTE LEVERANDØR
En leverandør, der har en direkte aftale med en NIS 2-omfattet enhed, og som leverer produkter eller tjenester, der påvirker enhedens net- og informationssystemer.

DOKUMENTATION
Dokumentation er nedskrevne politikker og procedurer, som alle relevante medarbejdere i enhederne har adgang til. Det kan eksempelvis være i form af papirdokumenter, sider på enhedernes intranet eller i en vidensdatabase. Enhederne kan benytte sig af den metode og form, de i forvejen anvender til at opbevare og formidle deres procedurer og lignende.
I forbindelse med tilsyn kan dokumentation også antage andre former, som eksempelvis netværksovervågnings-logs, udskrift af adgangstilladelse, referater m.v.

Dokumentationen skal under alle omstændigheder kunne gøres tilgængelig for tilsynet, der har behov for adgang til data, dokumenter og oplysninger, som er nødvendige for udførelsen af tilsynsopgaven.

ENHED
En enhed er en virksomhed, forening, organisation eller offentlig myndighed mv. (juridisk person), som er tildelt et CVR-nummer.

For mere information se vejledning om anvendelsesområdet.

FORANSTALTNINGER
Tiltag, der fremmer sikkerhed, som både omfatter tekniske, operationelle og organisatoriske foranstaltninger, der fastholder og/eller ændrer en risiko. Der er oplistet ti minimumskrav til foranstaltninger i NIS 2-lovens § 6, stk. 1, litra 1–10.

FORTROLIGHED
Fortrolighed betyder, at information kun er tilgængelig for de personer, enheder eller systemer, der har de rette autorisationer. Det handler om at beskytte information mod uautoriseret adgang.

HÆNDELSE
En begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, herunder OT-systemer (Operational Technology), i fare (NIS 2-loven § 3, stk. 12). På engelsk ofte benævnt ”incident”.

INTEGRITET
Integritet betyder, at information er nøjagtig, komplet, pålidelig og uændret, medmindre det er godkendt af de rette personer. Det sikrer, at data ikke er blevet ændret, slettet eller manipuleret på en uautoriseret måde.

KLASSIFIKATION
Inddeling af information og systemer i henhold til organisationens informationssikkerhedsbehov på grundlag af fortrolighed, integritet, tilgængelighed og relevante krav fra interessenter.

KRYPTOGRAFI OG KRYPTERING
Kryptografi anvendes til at beskytte information mod uautoriseret adgang og manipulation. Kryptering er en praktisk anvendelse af kryptografi, hvor data omdannes til en form, der kun kan læses af autoriserede parter med den rette nøgle.

LEDELSESORGAN

a) For virksomheder omfattet af selskabsloven er ledelsesorganet:

I. bestyrelsen i selskaber, der har en direktion og en bestyrelse

II. direktionen i selskaber, der alene har en direktion

III. direktionen i selskaber, der både har en direktion og et tilsynsråd.

b) For virksomheder omfattet af lov om visse erhvervsdrivende virksomheder er ledelsesorganet:

I. bestyrelsen i selskaber, der har en direktion og en bestyrelse

II. direktionen i selskaber, der alene har en direktion

III. for de selskaber, der hverken har en bestyrelse eller en direktion, det ledelsesorgan, der har en kompetence, der svarer til den almindelige opfattelse af den kompetence, der tilkommer en bestyrelse eller en direktion.

c) For offentlige myndigheder er ledelsesorganet den øverste administrative ledelse i myndigheden.

NET- OG INFORMATIONSSYSTEM

Et net- og informationssystem er i NIS 2-loven defineret som:

a) Et elektronisk kommunikationsnet, hvorved forstås transmissionssystemer, uanset om de bygger på en permanent infrastruktur eller centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabel-systemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, samt kabel-tv-net, uanset hvilken type information der overføres.

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

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.

Eksempler på dette kan være it-systemer, OT-systemer, IoT-enheder og it infrastruktur-komponenter.

POLITIKKER

Dokumenterede og godkendte retningslinjer, der angiver enhedens overordnede tilgang til et givent område. Politikker kan have mange former og kan navngives forskelligt alt efter enhedernes størrelse, branche, behov m.v. De kan f.eks. kaldes "retningslinjer", "principper", "strategier" eller "politikudkast", så længe de tydeligt beskriver formål, rammer og ansvar og er kendt og godkendt af den relevante ledelse.

PROCEDURER
En fastlagt måde at gøre noget på, ofte reguleret ved hjælp af formelle dokumenterede regler.

REDUNDANS
Redundans referer til implementering af ekstra eller alternative systemer, komponenter eller ressourcer, der kan træde i kraft, hvis systemer svigter eller bliver kompromitteret. Eksempelvis kan det være at have spejlede servere, ekstra kommunikationskanaler, alternativ strømforsyning, alternative føringsveje for forsyning eller ekstra komponenter på lager.

RELEVANT LEDELSE
Person eller gruppe af personer, der har ansvaret for bestemte dele af enhedernes forretning, eksempelvis HR, it, salg mv.

SEKTORANSVARLIGE MYNDIGHEDER
Begrebet beskriver den myndighed, der har ansvaret for, og tilsynet med, de respektive specifikke sektorer. De sektoransvarlige myndigheder udpeges ved en bekendtgørelse, inden NIS 2-loven træder i kraft. I NIS 2-loven bruges begrebet "kompetente myndigheder". De to betegnelser har samme betydning og skal forstås på samme måde.

TILGÆNGELIGHED
Tilgængelighed betyder, at information og systemer er tilgængelige og operationelle, når de er nødvendige. Det indebærer, at systemer og data skal være beskyttet mod forstyrrelser, og at de skal kunne genoprettes hurtigt i tilfælde af nedbrud.

VÆSENTLIG HÆNDELSE
En hændelse, der:

- forårsager eller kan forårsage alvorlige driftsforstyrrelser eller økonomiske tab for den berørte enhed, eller
- kan påvirke andre personer eller organisationer ved at forårsage betydelig fysisk eller ikke fysisk skade.

FORMÅL MED VEJLEDNINGEN

Denne vejledning skal hjælpe med at udfolde de krav, der er til foranstaltninger i NIS 2-lovens § 6 stk. 1, litra 1-10.

NIS 2-lovens § 6, stk. 1 stiller krav til en række foranstaltninger til styring af cybersikkerhedsrisici (herefter foranstaltninger), som omfattede enheder skal implementere. Kravene gælder, uanset om de omfattede enheder selv driver og vedligeholder deres net- og informationssystemer eller outsourcer drift og vedligeholdelsen af dem. Denne vejledning er en hjælp til, hvad den enkelte enhed kan gøre for at overholde loven.

MÅLGRUPPE

Målgruppen for vejledningen er vigtige og væsentlige enheder (herefter benævnt enheder), der er omfattet af NIS 2-loven.

For mere information se vejledning om anvendelsesområdet, som beskriver emnets overordnede regler.

LÆSEVEJLEDNING

Denne vejledning omhandler de krav til foranstaltninger, der er beskrevet i NIS 2-loven[1].
I loven er kravene både beskrevet i § 6, stk. 1 og i lovbemærkningerne til § 6.
Derfor citeres både bestemmelsen og bemærkningerne hertil i denne vejledning hvor relevant.
Vejledningen følger den rækkefølge af foranstaltninger, som fremgår af lovens ordlyd.

NIS 2-loven gælder ikke for enheder, der er omfattet af lov om styrket beredskab i energisektoren og lov om sikkerhed og beredskab i telesektoren. NIS 2-loven gælder derudover ikke for enheder, der er udpeget i medfør af den sektorspecifikke implementering af NIS 2-direktivet for finanssektoren. I det omfang, en enhed leverer ydelser, der er omfattet af sektorlovgivningen på henholdsvis energi-, tele- og finanssektoren og en sektor, der er omfattet af NIS 2-loven, vil enheden udover at overholde sektorlovgivningen også skulle overholde NIS 2-loven. Derudover skal enheder være opmærksomme på, at de kan være underlagt sektorspecifikke regler, der skal følges. For digitale udbydere er der eksempelvis vedtaget en gennemførelsesforordning[2], der stiller konkrete krav til blandt andet den konkrete implementering af NIS 2-direktivets krav til foranstaltninger. Forordningen stiller højere krav end kravene i NIS 2-lovens § 6.

1 Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) af 1. juli 2025
2 Kommissionens gennemførelsesforordning (EU) 2024/2690 af 17. oktober 2024

RISIKOBASERET TILGANG

NIS 2-loven understreger, at enhederne skal anlægge en risikobaseret tilgang til sikkerheds-arbejdet, da de ikke alle er risikoeksponeret i samme grad. Det vil sige, at enheden skal implementere de foranstaltninger (tekniske, operationelle og organisatoriske), der vurderes nødvendige for at opnå et passende niveau af sikkerhed i forhold til levering af den eller de ydelser, som gør, at enheden er omfattet af NIS 2-loven. Enhedens foranstaltninger skal dog som minimum omfatte de foranstaltninger, der er beskrevet i NIS 2-loven. Derudover skal enheden, hvor det er relevant, implementere foranstaltninger, der reducerer risikoen for hændelser eller minimerer deres skadevirkning på eventuelle modtagere af deres tjenester og på eventuelle andre tjenester.

Da omfattede enheder skal implementere foranstaltninger ud fra en risikobaseret tilgang, kan der godt eksistere varierende sikkerhedsniveauer i forskellige dele af enhedens net- og informations-systemer. Den risikobaserede tilgang indebærer blandt andet, at enheden skal foretage en vurdering af systemernes kritiske betydning og de samfundsmæssige og økonomiske skader, som en hændelse i systemet hos enheden ville kunne medføre for Unionens indre marked. Dette afviger fra en mere traditionel betragtning på risikoappetit i forhold til enhedens økonomi, omdømme, ansvar over for bestyrelsen mv.

Det afgørende er derfor, at man forholder sig til alle enhedens net- og informationssystemer fra en risikobaseret tilgang og implementerer passende foranstaltninger på den baggrund. NIS 2-loven tager udgangspunkt i en risikostyring, der omfatter alle farer (all-hazards approach). Det betyder, at enheden skal tage højde for alle de trusler, den står overfor, og alle de sårbarheder, den har. Det kan være tekniske og menneskelige fejl, miljømæssige påvirkninger (eksempelvis skybrud m.v.) og direkte bevidste handlinger (eksempelvis cyberangreb).

KRAV OG ANBEFALINGER

I denne vejledning skelnes der mellem de dele af foranstaltningerne, der **skal** implementeres (et krav), de dele af foranstaltningerne der **bør** implementeres (en anbefaling), og de foranstaltninger, der **kan** implementeres (et forslag eller eksemplificering). Enheder skal kunne forelægge dokumentation for de foranstaltninger, der **skal** implementeres. For de dele af foranstaltninger, der **bør** implementeres, skal enheden over for den relevante tilsynsførende myndighed være i stand til at forklare, hvorfor de ikke har implementeret den pågældende foranstaltning. Denne vurdering skal tage hensyn til det aktuelle teknologiske stade, gennemførelsesomkostningerne og enhedens risici, herunder samfundsmæssige og økonomiske indvirkninger. For de dele af foranstaltningerne, der **kan** implementeres, kan enheden betragte dem som en mulig måde at implementere foranstaltninger i NIS 2-loven (§ 6).

Enhederne bliver underlagt tilsyn fra de sektoransvarlige myndigheder. De sektoransvarlige myndigheder vil forvente, at anbefalingerne i denne vejledning er fulgt, eller at enheden ud fra en vurdering af dens risiko har taget dokumenteret stilling til, at deres risikohåndtering er tilstrækkelig.

Foranstaltningerne kan ses som generel god praksis for styring af cyber- og informations-sikkerhedsrisici. For nogle enheder er foranstaltningerne, der er beskrevet i NIS 2-lovens § 6, stk. 1, allerede implementeret. NIS 2-implementeringen er dog en god anledning til, at enhederne genbesøger deres risikostyring, samtidig med at de implementerer processer for indberetning af hændelser og sårbarheder.

For mere information om sidstnævnte se vejledning om hændelsesunderretning.

STANDARDER

For at sikre en samordnet gennemførelse af NIS 2-direktivet tilskyndes medlemsstaterne til at basere sig på europæiske og internationale standarder og tekniske specifikationer, der er relevante for sikkerheden i net- og informationssystemer.

For lettere at kunne identificere sammenhængen mellem standarder og de foranstaltninger, der er beskrevet i NIS 2-loven, er der i hvert kapitel en liste over de afsnit i relevante europæiske og internationale standarder, der behandler tilsvarende foranstaltninger.

Hvis en enhed allerede anvender en standard, vil enheden derfor kunne kortlægge sit eksisterende cyber- og informationssikkerhedsarbejde i forhold til NIS 2-loven. Enheder, der ikke anvender standarder, vil kunne finde uddybende hjælp til måder at arbejde med NIS 2-lovens foranstaltninger på i standarder. Standardernes uddybninger er ikke med i denne vejledning, da NIS 2-loven tager udgangspunkt i en minimumsimplementering af NIS 2-direktivet.

Det skal understreges, at det at følge en standard er en hjælp til efterlevelse, men ikke i sig selv er en sikkerhed for, at man opfylder kravene.

De standarder, der er valgt at medtage i denne udgave af vejledningen, er:

- **DS/EN ISO/IEC 27001:2023** Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse – Ledelsessystemer for informationssikkerhed – Krav
- **NIST CSF 2.0** National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0
- **DS/IEC 62443-2-1:2011** Industrielle kommunikationsnetværk – Netværks- og systemsikkerhed – Del 2-1: Etablering af et sikkerhedsprogram til industrielle automations- og styringssystemer
- **DS/EN IEC 62443-3-3:2019** Industrielle kommunikationsnetværk – Netværks- og systemsikkerhed – Del 3-3: Systemsikkerhedskrav og sikkerhedsniveauer
- **EECC -** Guideline on security measures under the EECC, 4th Edition, 2021
- **ETSI EN 319 401** Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers V2.3.1, May 2021

Vejledningen er udarbejdet på baggrund af det eksisterende fortolkningsbidrag, som ENISA har udsendt til EU-medlemsstaternes myndigheder, og vil løbende kunne tilpasses i overensstemmelser hermed.

1. POLITIK FOR RISIKOSTYRING OG INFORMATIONSSYSTEMSIKKERHED

Det siger NIS 2-loven:

§ 6, stk. 1, nr. 1 *Politikker for risikoanalyse og informations-systemsikkerhed.*

Lovbemærkninger
Det foreslås i nr. 1, at foranstaltningerne skal omfatte eller tage højde for politikker for risikoanalyse og informationssystemsikkerhed.

Dette indebærer bl.a., at enheden skal udarbejde en politik for informations-sikkerhed, der fastlægger den overordnede ramme for implementering af foranstaltninger, jf. § 6, stk. 1, nr. 1-10, som understøtter sikkerheden i enhedens omfattede net - og informationssystemer. Enheder skal endvidere udarbejde en politik for risikostyring, som indeholder metoder til at identificere og adressere eventuelle risici.

A. POLITIK FOR INFORMATIONSSYSTEMSIKKERHED

Formål

En politik for informationssystemsikkerhed udstikker en enheds tilgang til styring af dens informationssystemsikkerhed og dens implementering, inklusiv tekniske, operationelle og organisatoriske aspekter.

Foranstaltning

Enheden skal udarbejde og implementere en politik for informationssystemsikkerhed i net- og informationssystemer.

Politikken skal ud fra en risikobaseret tilgang sikre et passende sikkerhedsniveau i forhold til enhedens formål og under hensyntagen til det aktuelle tekniske niveau, gennemførelses-omkostninger og risiciene mod sikkerheden i enhedens net- og informationssystemer, der kan forvolde skade på data og tjenester af samfundsmæssig betydning.

Politikken skal være passende i forhold til NIS 2-loven og de forretningsmæssige mål, enheden har sat sig for at nå. Politikken bør understøtte enhedens kerneaktiviteter og eventuelle værdier samt tage højde for de risici, der er relevante for enheden.

Politikken for informationssystemsikkerhed bør:

- fastsætte enhedens tilgang til styring af sikkerheden i deres net- og informationssystemer – altså den samlede ramme for, hvordan enheden adresserer og håndterer sikkerheden i sine net- og informationssystemer, både på strategisk og operationelt niveau
- inkludere målsætninger for cybersikkerhed – altså beskrivelser af, hvad enheden ønsker at opnå med sin cybersikkerhed
- inkludere en forpligtelse til at opfylde eventuelle krav i relation til cybersikkerhed, eksempelvis lovmæssige krav som GDPR
- inkludere en forpligtelse til fortsat forbedring af informationssystemsikkerhedspolitikken, hvor det vurderes at være relevant
- være tilgængelig som dokumentation for alle relevante interessenter.

Enheden kan derudover udarbejde eventuelle emnespecifikke politikker, hvor der er behov. Det kan eksempelvis være en politik for backup, en politik for adgangsstyring m.v. Emnespecifikke politikker skal være i overensstemmelse med politikken for informations-systemsikkerhed.

Dokumentation

Politikken for informationssystemsikkerhed bør ajourføres årligt og ved væsentlige ændringer af enhedens forretningsmæssige mål og i trusselsbilledet

Politikken for informationssystemsikkerhed skal være godkendt af enhedens ledelsesorgan. Eventuelle emnespecifikke politikker bør gennemgås af den relevante ledelse, og resultatet af gennemgang og eventuelle tilretninger rapporteres til enhedens ledelsesorgan.

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
5.2, 6.2, 9.3, A.5.1, A.5.4, A.5.36
NIST CSF 2.0
PR.AT-02, GV.PO-01 & 02, GV.OC-02 & 03, GV.RM-03, ID.IM-01, ID.IM-02, ID.IM-03 & ID.IM 04.
DS/IEC 62443
DS/IEC 62443-2-1:2011: 4.3.2.2.1, 4.3.2.2.2, 4.3.2.6
EECC
SO1
ETSI EN 319 401
REQ 6.1-02, REQ 6.1-06, REQ 6.1-07, REQ 6.1-08, REQ 6.3

B. POLITIK FOR RISIKOSTYRING

Formål

At udarbejde, dokumentere og kommunikere en politik for og metoder til identifikation, analyse, evaluering og håndtering af enhedens risici. Ved at etablere politikker og metoder sikres en ensartet og målrettet risikostyring på tværs af enheden.

Foranstaltning

Enheden skal etablere og vedligeholde en politik for passende risikostyring for at identificere og adressere alle de relevante risici, der er i forhold til sikkerheden i enhedens net- og informations-systemer. Enheden skal gennemføre og dokumentere risikovurderinger og implementere og regelmæssigt revurdere risikohåndteringsplanen. Resultatet af risikovurdering, den planlagte risikohåndtering og niveauet af de tilbageværende risici, skal accepteres af risikoejeren, primært i relation til samfundsrisici, med passende rapportering til enhedens ledelsesorgan.

Politikken for risikostyring bør i forlængelse heraf:

- fastlægge en risikostyringsproces
- være en integreret del af enhedens generelle risikostyring
- omfatte alle trusler og sikre, at risikostyring adresserer risici, der stammer fra tredje part, eksempelvis leverandører
- etablere og vedligeholde kriterier for risikoevaluering
- identificere risikoejere og dokumentere deres ansvar.

Politikken bør også indeholde metoder til risikovurdering og kan indeholde en beskrivelse af:

- hvordan enheden identificerer og dokumenterer risici mod net- og informationssystemer, inklusiv identifikation af single points of failures[3]
- hvordan risici mod sikkerheden i net- og informationssystemer analyseres (truslen, sandsynligheden, konsekvens, eksisterende foranstaltninger, risikostørrelse) under iagttagelse af cybertrusler og sårbarheder
- hvordan de identificerede risici evalueres på baggrund af de fastsatte kriterier
- hvordan enheden identificerer og prioriterer passende foranstaltninger under hensyntagen til risikovurderingen og foranstaltningernes effektivitet
- hvem der er ansvarlig for rettidigt at implementere de foranstaltninger, enheden har besluttet sig for
- hvordan enheden dokumenterer de valgte foranstaltninger og begrundelserne for accept af de risici, der eventuelt er tilbage.

[3] Single Point of Failure (SPOF) refererer til en ikke-redundant del af et større system, som kan forårsage et total nedbrud af hele systemet, hvis den fejler.

Dokumentation

Politikker for risikostyring bør ajourføres med planlagte intervaller og ved væsentlige ændringer af enhedens forretningsmæssige virksomhed og ændringer i enhedens sårbarheder og trusselsbillede.

Politikken for risikostyring skal være dokumenteret og godkendt af enhedens relevante ledelse.

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
6.1, 6.1.2, 6.1.3, 6.2, 8.2, 8.3, A.5.7, A.5.19, A.5.20, A.5.21.
NIST CSF 2.0
ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, GV.RM-01, GV.RM-03, GV. RM-06, GV.RR-03, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04.
DS/IEC 62443-2-1:2011
DS/IEC 62443-2-1:2011: 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.11, 4.2.3.12, 4.2.3.13, 4.3.2.4.3, 4.3.2.6.3, 4.3.4.2 IEC 62443-2-4: 2015 SP 02.01, 03.01 IEC/TR 62433-1-2
EECC
SO2, SO28
ETSI EN 319 401
REQ 5, Clause 6.3

2. Håndtering af hændelser

Det siger NIS 2-loven:

§ 6, stk. 1, nr. 2 *Håndtering af hændelser*

Det følger af det foreslåede nr. 2, at foranstaltningerne skal omfatte eller tage højde for håndtering af hændelser.

Dette indebærer bl.a., at enheder skal udarbejde procedurer for håndtering af hændelser. Enheder skal i fornødent omfang implementere logning og monitorering af uregelmæssigheder i enhedens net- og informationssystemer med henblik på at kunne identificere hændelser. Logdata skal derudover sikres mod manipulation og beskyttes mod uautoriseret adgang.

A. HÅNDTERING AF HÆNDELSER

Formål

At sikre, at enheden kan reagere hensigtsmæssigt på væsentlige hændelser for at minimere konsekvenserne. Det indebærer at begrænse skader på net- og informationssystemer samt kritiske tjenester, så truslens indvirkning begrænses. Herefter at enhedens almindelige drift bliver genoprettet.

Foranstaltning

Enheden skal udarbejde og implementere procedurer (eksempelvis i beredskabsplaner) for at kunne identificere, opdage, analysere og reagere på hændelser, herunder for at kunne genoprette sikker stabil drift samt håndtere underretningsforpligtelser ved væsentlige hændelser.

Enheden skal have, eller gennem aftaler med tredje part have adgang til, kompetencer, der kan sikre, at:

- enheden kan vurdere hændelser for at afgøre, om hændelserne er væsentlige. Hvis det vurderes at være en væsentlig hændelse, skal enheden være i stand til at bestemme, hvad hændelsen indebærer, og hvor alvorlig den er.

Enheden bør i fornødent omfang:

- definere roller, ansvar og procedurer for at forebygge, opdage, analysere, inddæmme eller reagere på, genoprette, dokumentere og rapportere væsentlige hændelser så hurtigt som muligt. Herunder kan enheden have kommunikationsplaner for ekstern og intern kommunikation, samt nødkommunikationssystemer[4]
- implementere en procedure, der gør det muligt for medarbejdere, leverandører og kunder at kunne indberette mistænkelige hændelser internt i enheden. Processen bør være så let som mulig, for at der ikke skal opstå barrierer for, at den bliver brugt
- reagere på hændelser rettidigt og i overensstemmelse med enhedens procedurer for hændelseshåndtering
- gennemføre en gennemgang efter en væsentlig hændelse og identificere den grundlæggende årsag til hændelsen. Det kan bidrage til at udlede de erfaringer, der kan reducere forekomsten og konsekvenserne af fremtidige hændelser.

Enheden bør med planlagte mellemrum teste deres procedurer for reaktion på hændelser for at undersøge, om procedurerne virker efter hensigten.

For mere information se vejledning om hændelsesunderretning.

Dokumentation

Procedure for håndtering af hændelser bør ajourføres med planlagte intervaller og ved væsentlige ændringer af enhedens forretningsmæssige mål og ændringer i enhedens og trusselsbillede.

Procedure for håndtering af hændelser skal være dokumenteret og godkendt af den relevante ledelse.

[4] se "10.b. Nødkommunikationssystemer"

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.5.24
NIST CSF 2.0
GV.SC-08. RS.MA-01, RS.MA-05, RS.MI-01, RS.MI-02, ID.IM-01, ID.IM-04
DS/IEC 62443
DS/IEC 62443-2-1:2011: 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.11, 4.2.3.12, 4.2.3.13, 4.3.2.4.3, 4.3.2.6.3, 4.3.4.2 IEC 62443-2-4: 2015 SP 02.01, 03.01 IEC/TR 62433-1-2
EECC
SO18
ETSI EN 319 401
REQ-7.9-06

B. LOGNING OG MONITORERING

Formål

At enheden er i stand til at opdage hændelser, der kan bringe data i fare, og reagere passende og derved i videst mulige omfang afværge skadesvirkningen af hændelsen. Logs anvendes også til at undersøge hændelsen efterfølgende.

Foranstaltning

Enheden skal i nødvendigt omfang have processer og bruge værktøjer til at monitorere og logge samt reagere på aktiviteter på deres netværk og i deres informationssystemer. Hermed bliver enheden i stand til at opdage eventuelle hændelser og reagere i overensstemmelse hermed for at afbøde virkningerne.

Monitorering bør så vidt muligt være automatiseret (f.eks. Intrusion Detection Systems) og kan udføres enten i realtid eller med regelmæssige intervaller, afhængigt af virksomhedens muligheder.

Enheden skal vedligeholde, dokumentere og gennemgå logfiler. Logs kan, afhængig af enhedens teknologiske stade og en risikobaseret tilgang, eksempelvis omfatte:

- udgående og indgående netværkstrafik
- oprettelse, ændring eller sletning af brugere og udvidelse af tilladelser
- adgang til systemer og applikationer
- privilegeret adgang til systemer og applikationer
- aktiviteter, der udføres af privilegerede konti
- adgang til og ændringer i kritiske konfigurations- og backupfiler
- hændelseslogfiler og logfiler fra sikkerhedsværktøjer, f.eks. antivirus, Intrusion Detection/Prevention System eller firewalls
- brug af systemressourcer samt deres ydeevne
- adgang til og brug af enhedens netværksudstyr og –komponenter
- fysisk adgang til enhedens faciliteter, eksempelvis elektroniske adgangskontrolsystemer (ADK)
- miljøhændelser, der kan påvirke enhedens netværk og informationssystemer negativt, som f.eks. oversvømmelsesalarmer.

Logfilerne kan i relevant omfang gennemgås – manuelt eller automatiseret – for at opdage usædvanlige eller uønskede tendenser, og derfor bør enheden definere passende tærskler for, hvornår der skal skrides ind. Hvis de definerede tærskelværdier overskrides, kan det eventuelt automatisk udløse en alarm. Det ansvarlige personale skal sikre, at der i tilfælde af en alarm iværksættes en passende reaktion.

Enheden bør opbevare og sikkerhedskopiere logfiler i en på forhånd fastsat periode. Opbevarings-perioden er afhængig af enhedens forretningsområde og risikobillede. Logdata skal sikres mod manipulation og beskyttes mod uautoriseret adgang mv.

De implementerede foranstaltninger bør f.eks. være i stand til at opdage netværksbaserede angreb baseret på unormale ind- eller udgående trafikmønstre og/eller DDoS-angreb (distributed denial of service) i tide.

Enheden bør sikre, at alle systemer har synkroniseret tid (tids-kilde) for at kunne sammenligne logs mellem systemer til vurdering af hændelser.

Enheden bør udarbejde og føre en liste over alle de aktiver, der logges. Monitorerings- og lognings-systemer kan eventuelt dubleres for at sikre monitoreringen af sikkerheden i de tjenester, enheden leverer. Cybersikkerheden i monitorerings- og logningssystemerne bør monitoreres uafhængigt af de systemer, de overvåger og logger.

Dokumentation

Procedurerne for logning og monitorering, samt listen over aktiver eller hændelser, der logges, bør gennemgås med planlagte intervaller, og når der sker ændringer, blandt andet i trusselsbilledet og ved kendte sårbarheder, eller i tilfælde af væsentlige hændelser.

Der bør føres dokumentation for, at gennemgangen af procedurerne finder sted på det planlagte tidspunkt.

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.8.15, A.8.16, A.8.17
NIST CSF 2.0
RS.AN-06, RS.AN-07, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04.
IEC 62443
DS/IEC 62443-2-1:2011: 4.3.4.5.4 IEC 62443-3-3:2013: SR 1.11, SR 1.12, SR 1.13, SR 22 RE 1, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 6.1
EECC
SO19
ETSI EN 319 401
REQ-7.9-01, REQ-7.9-02, REQ-7.9-03, REQ-7.9-04, REQ-7.9-09, REQ-7.9-12

3. DRIFTSKONTINUITET

Det siger NIS 2-loven:

§ 6, stk. 1, nr. 3 *Driftskontinuitet, herunder backup-styring og reetablering efter en katastrofe og krisestyring.*

Lovbemærkninger
Det foreslås i nr. 3, at foranstaltningerne skal omfatte eller tage højde for driftskontinuitet, herunder backup-styring og reetablering efter en katastrofe og krisestyring.

Dette indebærer, at enheder skal udarbejde procedurer til sikring af drifts-kontinuitet i tilfælde af en hændelse. På grundlag af enhedernes risikostyring, jf. nr. 2, og driftskontinuitets-procedure skal enheder således udarbejde procedurer for backupstyring og gendannelse af data. Enheder skal foretage en vurdering af behovet for at udarbejde en beredskabsplan for krisestyring og reetablering efter en katastrofe. Enheder skal foretage en vurdering af, om der er behov for at etablere redundans, nødstrømsforsyning, understøttende forsyning eller anden sikring med tilsvarende virkning for enhedens net- og informationssystemer.

A. DRIFTSKONTINUITET

Formål

At sikre, at enhedens drift kan opretholdes, og at cybersikkerheden bevares i tilfælde af en væsentlig hændelse eller krise, og at normal-drift kan genetableres, når hændelsen eller krisen er overstået.

Foranstaltning

Enheden skal udarbejde og vedligeholde procedurer, der sikrer driftskontinuitet i tilfælde af en sikkerhedshændelse, eksempelvis en plan for fortsat drift og en plan for genopretning efter en krise.

Enhedens drift skal kunne genoprettes i overensstemmelse med kontinuitetsplanen. Planen skal baseres på resultaterne af risikovurderingen og kan indeholde:

- formål, omfang og målgruppe for kontinuitetsplanen
- roller og ansvar i tilfælde af en krise
- nøglekontakter (interne og eksterne, eksempelvis kontaktinformationer til driftsleverandører) og overblik over kommunikationskanaler, der kan anvendes
- betingelser for aktivering og deaktivering af enhedens beredskab
- en beskrivelse af de ressourcer, herunder backup, genindlæsning og redundans, der er behov for til at sikre driften i en krisesituation

- en beskrivelse af, hvordan samarbejdet skal være med dem, der tager sig af hændelseshåndteringen, eksempelvis hvad driften kan gøre under en hændelse, uden at det influerer negativt på inddæmning af hackere.

Planen for genopretning kan eksempelvis indeholde:

- genoprettelsesplaner for specifikke driftssystemer og genopretningsmål, eksempelvis hvor godt systemerne skal virke, og hvilke data der først skal være tilgængelige – dette kan f.eks. være en beslutning om, at mailsystemet skal i drift før, at filserverne er tilgængelige
- rækkefølge for genoprettelse af enhedens drift, eksempelvis hvilke tjenester der skal genoprettes før andre som følge af indbyrdes afhængigheder, en beskrivelse af genopretning og genstart af aktiviteter ved hjælp af midlertidige foranstaltninger, hvis sådanne findes – eksempelvis midlertidige arbejdsprocesser såsom manuelle arbejdsprocesser eller alternative kommunikationsformer
- en plan for, hvordan enheden verificerer, at der ikke har været brud på fortrolighed og integritet under genopretningen.

Dokumentation

Planer for opretholdelse af driften bør gennemgås og testes med regelmæssige planlagte mellemrum samt efter væsentlige hændelser og større ændringer i driftsmiljøet eller ændring i risici. Her bør det vurderes, om planerne virker efter hensigten og er tilstrækkelige og tidssvarende i forhold til enhedens aktuelle forhold.

Ændringer i planerne bør dokumenteres.

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.5.29, A.5.30
NIST CSF 2.0
ID.IM-02, ID.IM-03, ID.IM-04, GV.OC-04, GV.SC-08, RC.RP-01. RC.RP-02
IEC 62443
DS/IEC 62443-2-1:2011 4.3.2.5 IEC 62443-3-3:2013 SR7.1, SR7.2, SR7.4.
EECC
SO21, SO22
ETSI EN 319 401
Clause 7.11

B. BACKUP

Formål

At sikre, at der tages backup af enhedens relevante data, så data kan gendannes i tilfælde af tab, beskadigelse eller anden form for forstyrrelse af enhedens data.

Foranstaltning

Enheden skal etablere procedurer, der sikrer, at der tages backup af alle enhedens relevante data, herunder konfigurationsdata, i det omfang som enheden finder det nødvendigt for at opretholde sine tjenester.

Afhængig af risikovurderingen og planer for driftskontinuitet kan enhedens backupplaner tage hensyn til:

- reetableringstider, eksempelvis hvor lang tid det må tage at få data fra backup tilbage i almindelig drift
- sikkerhed for, at backups er fuldstændige og nøjagtige og omfatter konfigurationsdata og data, der opbevares i cloud-tjenestemiljøet
- lagring (online eller offline) af backupkopierne på et eller flere sikre steder, som ikke befinder sig i samme netværk som systemet (f.eks. air-gapped), og som befinder sig i tilstrækkelig afstand til at undgå enhver skade fra en hændelse på hovedstedet
- en passende fysisk og logisk kontrol med adgang til backups også under transport i overensstemmelse med aktivernes klassifikationsniveau (f.eks. aflåste serverrum med adgangskontrol, sikker fysisk transport med forsegling, krypterede backups med ekstern nøglestyring, RBAC (role-based access) eller multifaktorautentificering (MFA) på backupadgang
- hvilken opbevaringsperiode, der er behov for, baseret på forretningsmæssige, juridiske og regulatoriske krav
- hvornår og hvordan der må gendannes data fra backupkopierne (herunder godkendelses-processer)
- at der foretages regelmæssige tjek og tests af backup-kopiernes rigtighed og fuldstændighed (integritet), og at de kan genskabes
- jævnlige test af backup og procedurer for gendannelse.

I OT-miljøer, hvor oppetid er kritisk, kan alternative gendannelsesmetoder (f.eks. kopi af konfigurationsfiler til reetablering, system-redundans eller hurtig failover til prækonfigurerede enheder) også accepteres, forudsat at de understøtter kravet om driftskontinuitet.

Dokumentation

Enheden bør dokumentere, at den med jævne mellemrum tester, at dennes backup, eller alternative gendannelsesmetoder, er fuldstændig og tilgængelig i forhold til det, der er beskrevet i procedurer for backup, og at backuppen har den fornødne integritet, også selvom det ser ud til, at backup er fuldstændig.

Resultatet af tests bør dokumenteres og godkendes af den relevante ledelse.

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.8.13
NIST CSF 2.0
PR.DS-11, RC.RP-01, RC.RP-02, ID.IM-03
IEC 62443
DS/IEC 62443-2-1:2011: 4.3.2.5 IEC 62443-3-3:2013: SR 7.3 IEC 62443-2-4:2015: SP 12
EECC
SO10, SO22
ETSI EN 319 401
-

C. REDUNDANS

Formål

At sikre, at enheden har adgang til tilstrækkelige ressourcer, herunder faciliteter, personale, net- og informationssystemer og komponenter, når det er nødvendigt.

Foranstaltning

Enheden skal vurdere, om der er behov for at etablere redundans ved eksempelvis at have it-udstyr eller alternative lokationer i reserve. Vurderingen bør tage udgangspunkt i enhedens politikker for informationssystemsikkerhed og risikostyring samt kontinuitetsplan. Vurder bl.a. behovet for redundans ved hjælp af:

- net- og informationssystemer, dvs. hardware, software, tjenester, data osv. (f.eks. redundante netværksenheder, servere med belastningsbalancering, raid-arrays, backup-tjenester, flere datacentre og nødkommunikationssystemer[5])
- ikke-menneskelige aktiver, herunder faciliteter (eksempelvis lokaler), udstyr (eksempelvis værktøj) og forsyninger (eksempelvis nødstrøm)
- personale med det nødvendige ansvar, bemyndigelse og kompetence
- passende supplerende eller alternative kommunikationskanaler.

Enheden kan selv opbygge sin egen redundans eller indgå aftaler med tredjeparter for at tilvejebringe en passende redundans.

Enheden bør sikre, at de, der varetager overvågning og styring af ressourcer, herunder faciliteter, systemer og medarbejdere, er informeret om redundanskrav, så forventningerne er entydige, og de ansvarlige kan sikre de nødvendige ressourcer.

[5] se "10.b. Nødkommunikationssystemer"

Dokumentation

Enheden bør med regelmæssige planlagte mellemrum vurdere sit behov for redundans af hardware, software, tjenester, faciliteter mv. for at sikre, at de passende ressourcer er til stede i tilfælde af driftsforstyrrelser.

Anvendelse af enhedens redundante ressourcer bør være dokumenteret, så relevante medarbejdere har kendskab til, hvordan de ekstra ressourcer kan tilgås.

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.8.13, A.8.14
NIST CSF 2.0
PR.DS-11, RC.RP-01, RC.RP-02, ID.IM-03
IEC 62443
IEC 62443-2-1:2010 4.3.2.5, IEC 62443-3-3:2013 SR 7.3 IEC 62443-2-4: 2015 SP 12
EECC
SO10, SO22
ETSI EN 319 401
-

D. KRISESTYRING

Formål

At sikre, at enheden har processer på plads til at håndtere kriser i tilfælde af en eller flere samtidige væsentlige hændelser.

Foranstaltning

Enheden skal foretage en vurdering af behovet for at udarbejde en beredskabsplan med procedurer for krisestyring. Hvis enheden vurderer, at der er behov, bør enheden etablere og dokumentere de relevante procedurer til at håndtere særligt væsentlige hændelser.

Enheden kan eksempelvis sikre, at krisestyringsproducer adresserer følgende:

- opretholdelse af cybersikkerhed i en krise ved hjælp af passende foranstaltninger såsom brug af hjælpesystemer, processer og ekstra kapacitet
- roller og ansvar for medarbejdere, og hvor det er relevant, leverandører og tjeneste-udbydere, så det sikres, at de kender deres rolle i en krisesituation, herunder hvilke specifikke procedurer de skal følge

- passende kommunikationsmidler/kanaler mellem enheden og relevante sektoransvarlige myndigheder[6]. Denne kommunikation skal inkludere både obligatorisk kommunikation, såsom hændelsesunderretning inden for de obligatoriske tidsfrister og anden relevant kommunikation.

Enheden bør implementere en proces til at håndtere og anvende informationer om eksempelvis sikkerhedshændelser, sårbarheder, trusler og foranstaltninger, der modtages fra den nationale CSIRT, eller hvor relevant, den sektoransvarlige myndighed.

Dokumentation

Den dokumenterede plan for krisestyring bør gennemgås med regelmæssige planlagte mellemrum, hvor det bør vurderes, om planen er tilstrækkelig og tidssvarende i forhold til enhedens aktuelle forhold.

Der bør regelmæssigt gennemføres øvelser, der kan belyse, om planen for krisestyring virker efter hensigten, og efterfølgende bør de ændringer til planen, det findes nødvendige, implementeres og dokumenteres.

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.5.26, A.5.29, A.5.30
NIST CSF 2.0
RS.CO-02, RS.CO-03, PR.IR-03, DE.CM-01, ID.AM-03, DE.AE-02, DE.AE-03, DE.AE-04, DE.AE06, DE.AE-07, DE.AE-08
IEC 62443
DS/IEC 62443-2-1:2011: 4.3.2.5.6, A.3.4.5.5.2
EECC
-
ETSI EN 319 401
Clause 7.11

[6] Se ”10.b. Nødkommunikationssystemer”

EKSEMPEL PÅ RELEVANTE OVERVEJELSER OM DRIFTSKONTINUITET I EN OMFATTET ENHED (1/2)

En produktionsvirksomhed med automatiseret produktion og afhængighed af it- og OT-systemer er underlagt NIS 2-loven grundet virksomhedens rolle i samfundskritisk forsyning. Nedenfor nævnes en række centrale overvejelser vedrørende driftskontinuitet, backup, redundans og krisestyring.

Driftskontinuitet

- Hvilke systemer (f.eks. SCADA, ERP, produktionsstyring) er nødvendige for, at virksomheden kan opretholde de samfundskritiske funktioner, og hvilke afhængigheder findes der mellem systemerne?
- Hvordan kan virksomheden sikre opretholdelse af minimumsdrift i tilfælde af en hændelse?
- Hvilke manuelle processer eller midlertidige løsninger er realistiske?
- Hvordan organiserer virksomheden ansvar og kommunikation, så beslutninger kan træffes hurtigt i en krisesituation?
- Hvornår og hvordan skal kontinuitetsplanen testes og revideres?

Backup

- Hvilke data og systemer er det afgørende at kunne gendanne hurtigt – og i hvilken rækkefølge?
- Hvordan sikrer virksomheden, at deres backup-løsning er beskyttet mod både tekniske fejl og cyberangreb (f.eks. ransomware)?
- Hvordan sikrer virksomheden opbevaring af backup (skal der eksempelvis være fysisk og/eller logisk adskillelse)?
- Hvordan verificerer virksomheden, at deres backups er intakte og kan gendannes?
- Hvor lang tid er acceptabel for gendannelse af driftskritiske systemer (RTO)?

EKSEMPEL FORTSAT (2/2)

Redundans

- Hvor er virksomheden mest sårbar i forhold til single points of failure?
- Hvilke systemer eller processer kræver teknisk eller organisatorisk redundans for at opretholde driften?
- Kan produktionen fortsætte midlertidigt med reduceret kapacitet ved eksempelvis systemfejl eller strømudfald?
- Hvilke roller i virksomheden kræver backup-personale for at sikre håndtering af hændelser, også under pres?
- Har virksomheden alternative kommunikationskanaler til rådighed ved netværks- eller systemnedbrud?

Krisestyring

- Hvordan sikrer virksomheden hurtig mobilisering og klar rollefordeling ved en væsentlig hændelse?
- Hvilken information skal virksomheden dele internt og eksternt – og gennem hvilke kanaler?
- Er virksomheden i stand til at overholde NIS 2-lovens krav om underretning?
- Hvordan sikrer virksomheden, at alle nøgleaktører (ledelse, it, produktion) er forberedt og trænet i krisehåndtering?
- Hvordan integrerer virksomheden erfaringer fra tidligere hændelser, informationer fra myndigheder og trusselsvurderinger i deres krisestyring?

4. FORSYNINGSKÆDESIKKERHED

Det siger NIS 2-loven:

§ 6, stk. 1, nr. 4 *Forsyningskædesikkerhed, herunder sikkerheds-relaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.*

Lovbemærkninger
Det foreslås i nr. 4, at foranstaltninger skal omfatte eller tage højde for forsynings-sikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere. Dette indebærer, at enheder skal udarbejde procedurer for leverandørstyring for at sikre passende forsyningskædesikkerhed. […]

[…] Væsentlige og vigtige enheder bør derfor vurdere og tage hensyn til den generelle kvalitet og modstandsdygtighed af produkter og tjenester, de heri integrerede foranstaltninger til styring af cybersikkerhedsrisici og deres leverandørers og tjenesteudbyderes cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer. Væsentlige og vigtige enheder bør navnlig tilskyndes til at indarbejde foranstaltninger til styring af cybersikkerhedsrisici i kontraktlige arrangementer med deres direkte leverandører og tjenesteudbydere. Disse enheder kunne overveje risici hidrørende fra leverandører og tjenesteudbydere i andre led.

I overensstemmelse hermed bør procedurer efter det foreslåede nr. 4, tage højde for sikkerhedsrelaterede aspekter vedrørende forholdet mellem enheden og dens direkte leverandører og tjenesteudbydere relateret til enhedens net- og informations-systemer. Enheder skal i den forbindelse bl.a. udarbejde procedurer for aftaleindgåelse med direkte leverandører og tjenesteudbydere af produkter og tjenester, der kan påvirke sikkerheden i enhedens net -og informationssystemer.

Formål
At sikre, at leverandører og tjenesteudbydere opfylder enhedens behov for forsyningssikkerhed og krav til cybersikkerhed, så enheden og enhedens produkter eller tjenester ikke påvirkes negativt af sårbarheder eller hændelser hos enhedens leverandører eller i deres produkter/tjenester.

Foranstaltning
Enheden skal implementere procedurer for leverandørstyring, der sikrer både forsyningssikkerhed og cybersikkerhed i samarbejdet med direkte leverandører eller tjenesteudbydere - i det omfang deres ydelser kan påvirke sikkerheden i forhold til den eller de ydelser, som gør, at enheden er omfattet af NIS 2.

Det gælder både ved levering af it-produkter og tjenester samt andre kritiske leverancer som strøm, teknisk bistand med mere. Procedurerne skal gøre enheden i stand til at identificere og vurdere risici ved specifikke leverandører og indgå aftaler, der sikrer overholdelse af enhedens krav til forsynings- og cybersikkerhed.

For at undgå unødigt høje krav bør enheden anvende en risikobaseret tilgang, hvor kravene til den enkelte leverandør eller tjenesteudbyder er proportional med den specifikke leverances betydning for enhedens forsynings- og cybersikkerhed.

Enheden bør definere kriterier for, hvordan de udvælger leverandører eller tjenesteudbydere. Kriterierne kan omfatte:

- leverandørernes og tjenesteudbydernes cybersikkerhedspraksis, herunder deres procedurer for sikker udvikling
- leverandørens eller tjenesteudbyderens evne til at opfylde enhedens cybersikkerhedsspecifikationer
- klassifikationsniveau for de it-tjenester, it-systemer eller it-produkter, som leverandøren eller tjenesteudbyderen leverer, herunder leverandørens opfattelse af risikoen
- leverandøres evne til at opretholde et passende niveau af forsyningssikkerhed
- enhedens evne og mulighed for at vælge en alternativ leverandør og begrænse leverandørafhængighed
- leverandørens økonomi og geopolitiske risici.

Enheden bør sikre, at direkte leverandører og udbydere, herunder cloud computing-udbydere, opretholder passende foranstaltninger, der lever op til de sikkerhedskrav, enheden har fastlagt i kontrakten. Det kan ske gennem aftaler om serviceniveau (SLA) og/eller revisionsmekanismer.

I overensstemmelse med risikovurderingen kan aftaler (kontrakter) med direkte leverandører eller tjenesteudbydere eksempelvis indeholde afsnit om:

- krav om, at leverandøren og det leverede følger relevante sikkerhedskrav, lovkrav, eksempelvis fortrolighedsklausuler, standarder mv.
- hvilke færdigheder og eventuelle uddannelser, der kræves af leverandørens personale
- baggrundskontrol[7] af leverandørens personale, hvis de beskæftiger sig med enhedens kritiske aktiver (i henhold til klassificeringen af aktiver og risikovurderingen)
- leverandørens forpligtelse til at underrette enheden om alle relevante hændelser, så snart de bliver opmærksomme på hændelsen, og til at bistå enheden med at overholde sine rapporteringsforpligtelser i tilfælde af væsentlige hændelser
- at direkte leverandører og tjenesteudbydere, hvis enheden er underlagt tilsyn, samarbejder med enheden om at bistå de sektoransvarlige myndigheder i forbindelse med udførelsen af deres opgaver
- enhedens ret til revision og/eller ret til at modtage revisionsrapporter fra leverandøren
- aftale om leveringstider på serviceydelser, herunder eventuelle reparationer
- forpligtelse til at håndtere sårbarheder, der udgør en risiko for cybersikkerheden i enhedens net- og informationssystemer

[7] Se "9.a. Personalesikkerhed"

- underleverandører (hvis tilladt) og foranstaltninger for underleverandører
- leverandørens forpligtelser ved aftalens ophør, eksempelvis forpligtelse til at udlevere og bortskaffe data.

Enheden bør overveje at anvende disse sikkerhedskrav til eksisterende leverandører, som en del af udvælgelsesprocessen for nye direkte leverandører og udbydere, samt ved planlægning, forberedelse, styring og afslutning af indkøb af it-tjenester, it-systemer eller it-produkter.

Dokumentation

Enheden bør gennemgå procedurer til leverandørstyring og monitorere, gennemgå, evaluere og styre ændringer, der måtte opstå i de direkte leverandørers eller tjenesteudbyderes cybersikkerhedspraksis, med planlagte intervaller eller i tilfælde af en hændelse, der har eller kan påvirke cybersikkerheden i enhedens net- og informationssystemer. Observationer fra disse gennemgange, monitoreringer, evalueringer mv. bør dokumenteres.

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.5.19, A.5.20, A.5.21, A.8.30
NIST CSF 2.0
GV.OC-03, GV.OC-05, GV.SC-01, GV.SC-04, GV.SC.05 GV.SC-06, GV.SC-07, GV.SC-09, GV.SC-10, ID.RA-10, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04
IEC 62443
-
EECC
SO4
ETSI EN 319 401
Clause 7.1, 7.7

EKSEMPEL PÅ RELEVANTE OVERVEJELSER OM FORSYNINGSKÆDESIKKERHED I EN OMFATTET ENHED (1/2)

En dansk virksomhed er en væsentlig enhed under NIS 2-loven. Virksomheden er afhængig af automatiseret produktion, it- og OT-systemer samt en bred vifte af leverandører – herunder cloud- og serviceudbydere. Nedenfor nævnes en række centrale overvejelser vedrørende virksomhedens forsyningskædesikkerhed.

Identifikation og vurdering af leverandører

- Hvilke leverandører er kritiske for virksomhedens evne til at levere samfundsvigtige ydelser?
- Har virksomheden overblik over disse direkte leverandører, og har virksomheden behov for at kende leverandørers under-leverandører?
- Hvilke leverandører udgør en single point of failure i forsynings-kæden?
- Er leverandører af produktionsudstyr og automation sikkerheds-mæssigt vurderet? Eksempelvis på systemer med lang levetid, hvor der sjældent bliver opdateret firmware. Herunder også, hvordan det sikres, at leverandører, der opdaterer produktionssystemer, ikke utilsigtet bringer sårbarheder ind?
- Kan virksomheden skifte kritiske leverandører i tide ved f.eks. konkurs, opkøb eller sikkerhedsbrud? Har virksomheden alternative leverandører?

EKSEMPEL FORTSAT (2/2)

Etablering af aftalegrundlag

- Hvilke minimumskrav til cybersikkerhed og til håndtering af hændelser bør gælde for leverandører med adgang til virksomhedens systemer eller data?
- Er leverandørernes adgang passende segmenteret og kontrolleret? Er der brugt principper som least privilege, zero trust og time-bound access for eksterne parter?
- Hvordan sikrer virksomheden, at kontrakter eksempelvis indeholder krav om:
  1. overholdelse af relevante sikkerhedskrav og lovkrav?
  2. at leverandører kan og vil rapportere relevante hændelser hurtigt nok til, at virksomheden overholder NIS 2-lovens rapporteringspligt?
  3. ret til audit og dokumentation for sikkerhedspraksis, især for leverandører med adgang til produktionssystemer eller sensitive data?
  4. hvad leverandøren skal gøre ved kontraktens ophør, f.eks. i forhold til data?

Løbende styring og opfølgning

- Hvordan vurderer og overvåger virksomheden løbende leverandørers sikkerhedsniveau?
- Har virksomheden en plan for regelmæssig revurdering, f.eks. årligt eller ved ændringer hos leverandøren?

Hændelseshåndtering og kriseberedskab

- Har virksomheden klare kommunikationskanaler og kontaktpunkter til nøgleleverandører ved hændelser?
- Er leverandører inkluderet i virksomhedens kriseberedskab, herunder øvelser, og ved leverandører, hvad de skal gøre i tilfælde af en hændelse?

5. ERHVERVELSE, UDVIKLING OG VEDLIGEHOLDELSE

Det siger NIS 2-loven:

§ 6, stk. 1, nr. 5 *Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.*

Lovbemærkninger
Det foreslås i nr. 5, at foranstaltninger skal omfatte eller tage højde for sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.

Dette indebærer, at enheder skal udarbejde procedurer for sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af enhedens net- og informationssystemer, med udgangspunkt i politikken for informations-systemsikkerhed. Enheder skal endvidere udarbejde procedurer for håndtering af sårbarheder, der kan have indvirkning på enhedens net- og informationssystemer.

A. ERHVERVELSE, UDVIKLING OG VEDLIGEHOLDELSE

Formål

At planlægge, implementere og vedligeholde cybersikkerheden i hele et net- og informations-systems levetid – gennem hele livcyklussen (anskaffelse, implementering/indfasning, drift, udfasning og terminering/bortskaffelse) for de enkelte komponenter.

Foranstaltning

Enheden skal udarbejde dokumenterede procedurer for cybersikkerhed:

- ved anskaffelse af it-produkter eller tjenester fra tredje part
- ved udvikling af net- og informationssystemer
- ved vedligeholdelse af net- og informationssystemer
- ved afvikling/bortskaffelse af net- og informationssystemer.

Procedurerne skal tage udgangspunkt i enhedens politik for informationssystemssikkerhed og bør være koblet til enhedens politik og metoder for risikostyring samt procedurer for leverandørstyring[8].

[8] Se "1.a Politik for informationssystemssikkerhed", "1.b Politik for risikostyring" og "4. Forsyningskædesikkerhed"

Enheden kan:

- sikre, at sikkerhedsopdateringer er tilgængelige fra producenten i hele produktets forventede levetid
- etablere, dokumentere, implementere og overvåge konfigurationer, herunder patches og opdateringer af hardware, software, tjenester og netværk i egenudviklede såvel som indkøbte net- og informationssystemer
- sikre, at ændringer, reparationer og vedligeholdelse af net- og informationssystemer er underlagt procedurer for ændringsstyring i overensstemmelse med enhedens politikker
- udføre tests, der kan spænde fra konfigurationsgennemgange til tests af enhedens samlede net- og infrmationssikkerhed[9]
- specificere og anvende procedurer for ændringsstyring
- styre risici, der stammer fra erhvervelse af it-tjenester, it-systemer eller it-produkter fra leverandører og tjenesteudbydere gennem hele tjenestens, systemets eller produktets livscyklus[10]
- etablere og stille tydelige krav om at anvende regler for sikker udvikling af software og systemer, når enheden anskaffer eller udvikler net- og informationssystemer. Reglerne bør dække alle udviklingsfaser (specifikation, design, udvikling, implementering og test), eksempelvis gennem "Security by Design"[11]
- adskille systemer i netværk eller zoner baseret på forretningsbehov og kritikalitet under hensyntagen til resultaterne af risikovurderinger
- beskytte net- og informationssystemer mod skadelig og uautoriseret software ved at indføre foranstaltninger, der detekterer eller forhindrer brugen af malware - eksempelvis ved at installere og opdatere automatisk anti-malware-software på alle relevante aktiver.

Dokumentation

Enheden bør gennemgå deres processer for styring af livscyklus for indkøbte og selvudviklede it-tjenester, it-systemer eller it-produkter med regelmæssige planlagte mellemrum eller ved væsentlige hændelser. Observationer fra gennemgangen bør dokumenteres.

[9] Se "6.b Tekniske tests"
[10] Se "4. Forsyningskædesikkerhed"
[11] Produkter med digitale elementer vil snart skulle leve op til kravene i EU's forordning (2024/2847) - Cyber Resilience Act (CRA). Formålet med forordningen er at sikre horisontale cybersikkerhedskrav til produkter med digitale elementer, så digitale produkter er designet, udviklet og vedligeholdt med et højt cybersikkerhedsniveau i hele deres levetid. Kravene gælder også i Danmark. Forordningen er trådt i kraft, men bliver gradvist implementeret frem til december 2027.

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
6.3, 8.1, A.5.21, A.5.23, A.5.32, A.7.13, A.8.7, A.8.9, A.8.16, A.8.20, A.8,22, A.8.25, A8.31, A.8.32
NIST CSF 2.0
GV.PO-02, GV.SC-06, PR.IR-01, PR.PS-01, PR.PS-02, PR.PS-05, PR.PS-06, DE.CM-01, DE.CM-09, ID.AM-08, ID.RA-07, ID.RA-09, ID.RA-10, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04
IEC 62443
IEC 62443-2-1:2010 4.2.3.5, 4.3.4.3, 4.3.4.3.1, 4.3.4.3.2, 4.3.4.3.3, 4.3.4.3.4, 4.3.4.3.5, IEC 62443-3-3:2013 SR1.11, SR1.12, SR1.13, SR2.5, SR2.6, SR2.7, SR3.1, SR3.2, SR3.3, SR 3.4, SR 3.5, SR3.8, SR5.2, SR 7.6, SR7.7, IEC 62443-2-4:2015
EECC
SO4, SO11, SO12, SO16, SO17, SO25, SO26
ETSI EN 319 401
REQ-6.3-09, REQ-7.7-01, REQ-7.7-02, REQ-7.7-03, REQ-7.7-04, REQ-7.7-05, REQ-7.7-09, REQ-7.8, REQ-7.8-02, REQ-7.8-10

B. HÅNDTERING AF SÅRBARHEDER

Formål

At enheden er orienteret om eventuelle sårbarheder og kan implementere passende foranstaltninger, der nedsætter sandsynligheden for, at sårbarhederne kan udnyttes. Derudover kan videregivelse af informationer om sårbarheder hjælpe andre til at blive opmærksomme på eventuelle sårbarheder i deres net- og informationssystemer.

Foranstaltning

Enheden skal udarbejde procedurer for håndtering af sårbarheder, der kan have indvirkning på enhedens net- og informationssystemer. Procedurerne skal gøre enheden i stand til at indhente oplysninger om tekniske sårbarheder i sine net- og informationssystemer, evaluere enhedens eksponering for sådanne sårbarheder og træffe passende foranstaltninger til at håndtere sårbarhederne.

Enheden bør:

- følge med i informationer om sårbarheder fra forskellige kilder. Eksempelvis i meddelelser fra CSIRT, den sektoransvarlige myndighed eller i informationer modtaget fra leverandører eller tjenesteudbydere
- implementere proceduren for håndtering af sårbarheder eller dokumentere begrundelsen for, hvorfor en sårbarhed ikke kræver udbedring.

Enheden bør udføre sårbarhedsscanninger med regelmæssige planlagte mellemrum og ved større ændringer eller sikkerhedshændelser, og dokumentere resultaterne[12]. Vær opmærksom på, at aktive scanninger af OT-miljøer kan medføre forstyrrelser eller nedetid. Som alternativ til aktive sårbarhedsscanninger i OT-miljøer kan enheden implementere passive overvågningsmetoder, som f.eks. monitorering og netværkstrafikanalyse, der kan være understøttet af regelmæssige sikkerhedsvurderinger af systemkonfigurationer.

Håndteringen af sårbarheder bør være afstemt med enhedens styring af ændringer og håndtering af hændelser. Sårbarheder, der anses for at være kritiske, bør håndteres uden unødige forsinkelser.

Enheden kan have en politik for koordineret offentliggørelse af sårbarheder (Coordinated Vulnerability Disclosure - CVD), som dækker egne net- og informationssystemer.

Enheden skal indberette væsentlige hændelser.

For mere information se vejledning om hændelsesunderretning. Sårbarheder, der endnu ikke er offentligt kendte, bør videregives til den udpegede CSIRT, hvor det er relevant.

Dokumentation

Enheden bør gennemføre sårbarhedsscanninger og indsamle observationer med regelmæssige planlagte mellemrum og ved større ændringer eller sikkerhedshændelser. Scanninger, observationer og håndtering bør dokumenteres.

Enheden bør monitorere sine kilder til sårbarhedsinformationer med planlagte mellemrum og dokumentere de sårbarheder, der er relevante for enheden.

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.8.8, A.5.7, A.8.20, A.8.21, A.8.25, A.8.26, A.8.27, A.8.28, A.8.29
NIST CSF 2.0
ID.RA-1, ID.RA-02, ID.RA-04, ID.RA-05, ID.RA-06, ID.RA-08, PR.PS-02, PR.PS-03, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04
IEC 62443
IEC 62443-2-1:2010 4.2.3.7, 4.2.3.14, IEC TR 62443-2-3, IEC 62443-2-4: 2015 SP 02.02 RE(2), SP 03.03
EECC
SO12, SO26, SO28
ETSI EN 319 401
REQ-7.8-13, REQ-7.8-13A, REQ-7.9-10, REQ-7.9-11

[12] Se ”6.b. Tekniske tests”

6. EFFEKTIVITET AF FORANSTALTNINGER

Det siger NIS 2-loven:

§ 6, stk. 1, nr. 6 *Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.*

Lovbemærkninger
Det foreslås med nr. 6, at foranstaltninger skal omfatte eller tage højde for politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.

Dette indebærer, at enheder skal udarbejde en politik og procedurer med henblik på at vurdere effektiviteten af de implementerede foranstaltninger samt for vurdering af behov for tekniske tests for potentielle sårbarheder, herunder f.eks. i form af sårbarhedsscanninger eller penetrationstests.

A. VURDERING AF EFFEKTIVITETEN AF DE IMPLEMENTEREDE FORANSTALTNINGER

Formål

At sikre, at de foranstaltninger, enheden implementerer, er tilstrækkelige i forhold til de risici, enheden står overfor. Foranstaltningerne skal være proportionale med både trusselsbilledet og de ressourcer, der er afsat til området.

Foranstaltning

Enheden skal udarbejde en politik for, hvordan man løbende vurderer enhedens implementerede foranstaltninger. Vurderingen skal undersøge, om foranstaltningerne er tilstrækkelige til fortsat at beskytte mod relevante risici samt vurdere, om enhedens politik for informationssystemsikkerhed[13] er i overensstemmelse med både enhedens egne krav, gældende lovgivning og relevante gennemførelsesforordninger[14].

Herudover skal enheden udarbejde procedurer for at gennemføre disse vurderinger samt vurdere behovet for tekniske tests.

[13] Se "1.a Politik for informationssystemssikkerhed
[14] I EU-regi er gennemførelsesforordninger (implementing acts) retsakter, som præciserer, hvordan EU-lovgivning skal anvendes i praksis. De vedtages af Europa-Kommissionen for at sikre ensartet gennemførelse af EU-regler i alle medlemslande. Gennemførelsesforordninger er bindende og gælder direkte i hele EU uden krav om national lovgivning. For digitale udbydere er der vedtaget en gennemførelsesforordning (EU) 2024/2690 af 17. oktober 2024

Procedurerne bør indeholde:

- konkrete værktøjer og metoder, der gør det muligt løbende at vurdere og afprøve sikkerheden i net- og informationssystemer, eksempelvis ved brug af tekniske tests[15]
- vurderingen af, om foranstaltninger lever op til gældende love og regler
- metoder til at vurdere, om politikken efterleves, samt hvordan enheden kontrollerer, at foranstaltningerne er implementeret effektivt og vedligeholdes i forhold til de aktiver, de skal beskytte
- en metode til håndtering af en foranstaltning, der vurderes ineffektiv, der sikrer, at der følges op, og at der ændres på foranstaltningen
- angivelse af, hvem der skal udføre vurderingerne.

Politik og procedurer bør tage højde for:

- resultater af risikovurderinger
- tidligere hændelser
- hvad foranstaltningerne skal beskytte, om foranstaltningerne giver den rette beskyttelse, og om enheden har de nødvendige driftsbetingelser til at afvikle foranstaltningerne.

Politik og procedurer bør være koblet til enhedens politik for informationssystemssikkerhed, enhedens politik og metoder for risikostyring, samt hændelseshåndtering[16].

Enheden kan sikre, at de personer, der har ansvar for risikostyring, foranstaltninger og ledelses-rapportering, er bekendt med kravene til vurdering af effektivitet, så de kan tilrettelægge relevante kontroller og følge op på resultaterne.

Dokumentation

Politik og procedure for vurdering af effektiviteten af de implementerede foranstaltninger bør ajourføres med planlagte intervaller og ved væsentlige ændringer af enhedens forretningsmæssige mål og ændringer i enhedens sårbarheder og trusselsbillede. Det kan eksempelvis være forud for den fastlagte gennemgang af enhedens politik for informationssystemsikkerhed.

[15] Se "6.b. Tekniske tests"
[16] Se "1.a Politik for informationssystemssikkerhed", "1.b Politik for risikostyring" og "2. Håndtering af hændelser"

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
6.2, 9.1, 9.3
NIST CSF 2.0
GV.RM-06, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04
IEC 62443
IEC 62443-2-1:2010 4.4.2.3, 4.4.3, IEC/TS 62443-1-3
EECC
-
ETSI EN 319 401
CLAUSE 5, REF. TIL ISO/IEC 27005:2011

B. TEKNISKE TESTS

Formål

Ved hjælp af tekniske tests er det muligt at teste for eventuelle sårbarheder og derved undersøge effektiviteten af de foranstaltninger, som enheden har implementeret.

Foranstaltning

Enheden skal løbende vurdere behovet for tekniske tests som led i evalueringen af, hvor effektivt de implementerede foranstaltninger fungerer[17].

På baggrund af en risikovurdering skal enheden definere behovet for og frekvensen af forskellige typer af tests, samt hvilke komponenter, systemer og organisatoriske elementer, der er relevante at teste i forhold til sikker drift.

Tekniske tests kan eksempelvis være:

- sårbarhedsscanninger (automatisk scanning for kendte sårbarheder i systemer, netværk og applikationer). Vær opmærksom på, at aktive scanninger af OT-miljøer kan medføre forstyrrelser eller nedetid[18]
- penetrationstests (pentests). Simulerede angreb for at identificere og udnytte sårbarheder, som en angriber ville kunne udnytte
- red team-tests (avancerede, målrettede angreb for at teste det samlede forsvar og detektionsevne)
- blue team-aktiviteter (forsvar og hændelseshåndtering mod angreb, inkl. logovervågning og respons[19])

[17] Se "6.a. Vurdering af effektiviteten af de implementerede foranstaltninger"
[18] Se "5.b. Håndtering af sårbarheder"
[19] Se "2. Håndtering af hændelser"

- konfigurationsgennemgang (review af system- og netværksopsætninger ift. best practice og sikkerhedspolitikker)
- kodegennemgang (analyse af kildekode for at identificere sikkerhedsfejl og svagheder)
- patch management review (gennemgang af opdateringsrutiner og om kendte sårbarheder er adresseret[20])
- social engineering-tests (tests af menneskelig sårbarhed via f.eks. phishing, smishing eller fysisk adgang)
- tests af adgangskontroller og passwordsikkerhed (kontrol af autentificeringsmekanismer, herunder styrken af adgangskoder[21]).

Net- og informationssystemer bør sikkerhedstestes i forbindelse med installation, vedligeholdelse samt ved opgradering eller ændringer af infrastruktur og applikationer, som enheden vurderer som væsentlige[22]. Derudover bør der gennemføres regelmæssige og planlagte tekniske tests på tværs af organisationen samt ved væsentlige ændringer. Test kan udføres af enheden eller af tredjepart. Tekniske tests kan udføres i henhold til en dokumenteret testmetodologi og dække de komponenter, der blev identificeret som relevante for sikker drift i risikoanalysen. Resultater af test bør noteres under testforløbet. Testenes type, omfang, tidspunkt og resultater bør dokumenteres, så de er forståelige for tredjeparts eksperter.

Resultaterne af tekniske tests kan, hvis det er relevant, bruges til at opdatere politikker og procedurer til at vurdere effektiviteten af sikkerhedsforanstaltninger[23].

Resultaterne af testene bør som minimum dokumenteres med en vurdering af, hvor kritiske testenes resultater er, og hvilke efterfølgende kompenserende handlinger der er udført, hvis resultaterne vurderes at kunne påvirke fortroligheden, integriteten, autenticiteten eller tilgængeligheden af de pågældende systemer negativt. Restrisiko skal accepteres af risikoejere med passende rapportering til relevant ledelse.

Dokumentation

Test bør gennemføres med passende planlagte mellemrum og ved større ændringer eller væsentlige hændelser.

Dokumentation fra tests bør gennemgås af relevant personale med passende planlagte mellemrum, og resultater bør rapporteres til relevant ledelse.

[20] Se "5.b. Håndtering af sårbarheder"
[21] Se "9.b. Adgangskontrol" og "10.a. Multifaktorautentificering"
[22] Se "5.a. Erhvervelse, udvikling og vedligeholdelse"
[23] Se "6.a. Vurdering af effektiviteten af de implementerede foranstaltninger"

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.8.29, A.8.33, A.8.34
NIST CSF 2.0
ID.RA-01, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04
IEC 62443
IEC 62443-2-1:2010 4.3.4.3.1, IEC 62443-3-3:2013 SR 3.5, SR 3.6, SR 3.7, IEC 62443-2-4:2015 SP 02.02 RE(3)
EECC
SO25
ETSI EN 319 401
REQ-7.8-10, REQ-7.8-14, 14A, REQ-7.8-15

7. CYBERHYGIEJNE OG CYBERSIKKERHEDSUDDANNELSE

Det siger NIS 2-loven:

§ 6, stk. 1, nr. 7 *Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.*

Lovbemærkninger
Det foreslås i nr. 7, at foranstaltninger skal omfatte eller tage højde for grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.

Dette indebærer bl.a., at enheder skal implementere relevante grundlæggende cyberhygiejnepraksisser med udgangspunkt i deres politik for informationssikkerhed, herunder f.eks. gennem brug af passwords og sikker brug af mails. Endvidere skal enheder udarbejde en politik for uddannelse af relevante medarbejdere for at sikre, at medarbejderne har relevant viden og færdigheder om informationssikkerhed.

A. CYBERHYGIEJNEPRAKSISSER

Formål

At opretholde et passende niveau af cybersikkerhed gennem implementering af fundamentale foranstaltninger.

Foranstaltning

Enheden skal implementere relevante grundlæggende cyberhygiejnepraksisser med udgangspunkt i enhedens politik for informationssystemsikkerhed[24]. Cyberhygiejne dækker over de grundlæggende foranstaltninger og daglige sikkerhedsvaner, praksisser og procedurer, som beskytter netværk, systemer og data mod almindelige trusler. Dette indebærer blandt andet implementeringen af en række fundamentale foranstaltninger.

Nedenfor er oplistet en række fundamentale foranstaltninger med henvisning til relaterede afsnit i denne vejledning.

[24] Se "1.a Politik for informationssystemssikkerhed"

Enheden bør:

- udarbejde et minimumssæt af grundlæggende sikkerhedspolitikker (se "1. Politik for risikoanalyse og informationssystemsikkerhed")
- regelmæssigt sikkerhedskopiere relevante data, teste sikkerhedskopierede data (integritetskontrol) og teste procedurerne for gendannelse af sikkerhedskopien (se "3.b. Backup")
- planlægge kapacitet og ressourcer (personale og it-ressourcer) for at undgå mulige kapacitetsflaskehalse (se "3.c. Redundans")
- udvikle en beredskabsplan for hændelser (se "3.d. Krisestyring")
- regelmæssigt evaluere cybersikkerheden i enhedens it-forsyningskæde (se "4. Forsyningskædesikkerhed")
- udarbejde risikobaserede aftaler for serviceniveau (SLA'er) med sine leverandører og tjenesteudbydere (se "4. Forsyningskædesikkerhed")
- regelmæssigt patche og opdatere operativsystemer og applikationer (se " 5.a. Erhvervelse, udvikling og vedligeholdelse")
- installere og opdatere automatisk anti-malware-software på alle relevante aktiver (se "5.a. Erhvervelse, udvikling og vedligeholdelse")
- segmentere enhedens netværk i henhold til aktivers kritikalitet (se "5.a. Erhvervelse, udvikling og vedligeholdelse")
- regelmæssigt udføre automatiserede sårbarhedsscanninger i enhedens netværks- og informationssystemer (se "6.b. Tekniske tests")
- udføre regelmæssige sikkerhedstests (se "6.b. Tekniske tests")
- udvikle cybersikkerhedskultur og -bevidsthed gennem regelmæssig brugertræning (se "7.b. Cybersikkerhedsuddannelse")
- kryptere data i hvile og i transit i overensstemmelse med aktivers klassifikationsniveau (se "8. Kryptografi")
- begrænse administrative rettigheder (se "9.b. Adgangskontrol")
- håndhæve stærke passwords (se "9.b. Adgangskontrol")
- bruge multifaktorautentificering (MFA) i overensstemmelse med aktivers klassifikationsniveau (se "9.b. Adgangskontrol")
- begrænse netværksporte og -tjenester til det absolut nødvendige for enhedens forretningsbehov (se " 9.b. Adgangskontrol")
- oprette en fortegnelse over hardware- og softwareaktiver (se " 9.c. Forvaltning af aktiver").

Dokumentation

Der henvises til relevant dokumentation beskrevet i de andre afsnit om de pågældende foranstaltninger.

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
7.3, A.6.3, A.8.7
NIST CSF 2.0
PR.AT-01, PR.AT-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04
IEC 62443
IEC 62443-2-1:2010 4.3.2.4, 4.3.4.5.5
EECC
SO6, SO29
ETSI EN 319 401
REQ-7.2-02, REQ-7.2-03, REQ-7.2-04

B. CYBERSIKKERHEDSUDDANNELSE

Formål

At sikre, at medarbejdere på alle niveauer er opmærksomme på, og er uddannet og trænet til at håndtere, relevante sikkerhedsrisici, samt kender og anvender almindelige cyberhygiejnepraksisser (se afsnittet overfor).

Foranstaltning

Enheden skal udarbejde en politik for uddannelse af medarbejdere for at sikre, at de modtager net- og informationssikkerhedstræning og uddannelse, der klæder medarbejderne på til at håndtere relevante sikkerhedsrisici og beskytte net- og informationssystemer. Uddannelse og træning skal etableres i overensstemmelse med enhedens politik for informations-systemsikkerhed[25], eventuelle emnespecifikke politikker og relevante procedurer for net- og informationssikkerhed.

Politikken kan eksempelvis indeholde beskrivelser af, hvilke arbejdsmæssige roller der kræver specifikke sikkerhedsrelevante færdigheder og ekspertise. Der kan etableres et egentligt uddannelses- og træningsprogram, som definerer den nødvendige uddannelse og træning for medarbejdere. Uddannelse og træning bør være relevant for medarbejderens jobfunktion, og programmets effektivitet bør vurderes.

[25] Se "1.a. Politik for informationssystemssikkerhed"

Uddannelse og træning bør ske regelmæssigt og være dokumenteret samt tage hensyn til generelle foranstaltninger og kan blandt andet omfatte:

- instruktioner i og træning af gængse cyberhygiejnepraksisser, som bruges i enheden, såsom adgangsstyring, håndtering af opdatering af f.eks. mobile enheder, brug af passwords mv.[26]
- løbende orientering om kendte trusler, der er relevante for enheden og for medarbejdere (orienter f.eks. om forskellige relevante angrebsmetoder eller menneskelige sårbarheder (menneskelige bias), og tilpas orienteringen til medarbejdernes roller)
- uddannelse og træning i, hvad medarbejdere skal gøre, når der indtræffer hændelser (gør træningen konkret og handlingsorienteret – brug f.eks. scenarier, der tager udgangspunkt i enhedens risikovurdering[27] og foranstaltninger).

Grunduddannelse kan gælde for nye medarbejdere og for dem, der overgår til nye stillinger eller roller med væsentligt anderledes krav til net- og informationssikkerhed.

Der er krav til, at ledelsesorganet skal deltage i relevante kurser, samt tilskynde til at tilsvarende kurser tilbydes til enhedens øvrige ansatte (NIS 2-loven § 7, stk. 2.).

For mere information om ledelsens rolle og opgaver, se vejledning om ledelsens rolle og opgaver.

Relevante kurser kan for eksempel være generelle kurser om cyber- og informations-sikkerhed, workshops om styring af cyber- og informationssikkerhedsrisici, kurser og certificeringer i anerkendte europæiske og internationale sikkerhedsstandarder eller enhedens egne internt tilrettelagte kurser og seminarer om cyber- og informations-sikkerhed.

Dokumentation

Uddannelses- og træningsprogram bør opdateres og gennemføres med regelmæssige mellemrum under hensyntagen til gældende politikker og regler, tildelte roller, ansvarsområder samt kendte trusler og teknologisk udvikling.

[26] Se f.eks. ”7.a. Cyberhygiejnepraksisser”
[27] Se ”1.b. Politik for risikostyring”

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
7.2, A.6.3
NIST CSF 2.0
PR.AT-01, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04
IEC 62443
IEC 62443-2-1:2010 4.3.2.4
EECC
SO6
ETSI EN 319 401
REQ-7.2-03

8. KRYPTOGRAFI

Det siger NIS 2-loven:

§ 6, stk. 1, nr. 8 *Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering.*

Lovbemærkninger
Det foreslås med nr. 8, at foranstaltninger skal omfatte eller tage højde for politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering.

Dette indebærer bl.a., at enheder skal udarbejde en politik og procedurer for brug af kryptografi og, hvor det er relevant, kryptering for at beskytte deres net- og informationssystemer. Politikken og procedurerne skal være passende i forhold til det aktuelle teknologiske stade.

Formål
At sikre tilstrækkelig og effektiv brug af kryptografi til at beskytte informationens fortrolighed, autenticitet og/eller integritet.

Foranstaltning
Enheden skal udarbejde og implementere en politik og procedurer vedrørende kryptografi med henblik på at sikre tilstrækkelig og effektiv brug af kryptografi til at beskytte informationens fortrolighed, autenticitet og/eller integritet i overensstemmelse med aktivernes klassifikations-niveau og resultaterne af risikovurderingen. Politikken og procedurerne skal være passende i forhold til det aktuelle teknologiske stade. Kryptografi kan bruges til forskellige formål, eksempelvis til opbevaring af password, sikker identifikation af data og dens validitet, samt beskyttelse af datas fortrolighed.

Enheden skal benytte kryptografi i beskyttelsen af net- og informationssystemer, hvor det er påkrævet i henhold til aktivers klassifikation og risikovurdering[28].

[28] Se "1.b. Politik for risikostyring" og "9.c. Forvaltning af aktiver"

Politikken og procedurerne for brug af kryptografi og kryptering i enheden kan eksempelvis omfatte:

- en beskrivelse af de protokoller, der må anvendes
- de kryptografiske algoritmer, der må anvendes (eksempelvis hvis enheden har en politik om at bruge specifikke anerkendte standarder til kryptering)
- nøglelængder, der må anvendes til de forskellige algoritmer
- kryptografiske løsninger og brugspraksis, der er godkendte, eller som det er et krav at bruge i enheden, f.eks. end-to-end-kryptering af kommunikation (eksempelvis VPN), harddiskkryptering af data osv.
- en beskrivelse af tilgangen til nøglehåndtering, herunder metoder til at:
    - generere nøgler til forskellige kryptografiske systemer og forskellige applikationer
    - udstede og erhverve offentlige nøglecertifikater
    - distribuere nøgler til de enheder, der skal anvende dem, herunder hvordan man aktiverer nøgler, når de er modtaget
    - opbevare nøgler, herunder hvordan autoriserede brugere får adgang til nøgler
    - ændre eller opdatere nøgler, herunder regler for, hvornår der skal skiftes nøgler, og hvordan det skal gøres
    - håndtere kompromitterede nøgler og certifikater
    - tilbagekalde nøgler, eksempelvis hvordan enheden kan trække nøgler tilbage eller deaktivere dem
    - gendanne nøgler, der er mistet eller beskadiget
    - backup eller arkivering af nøgler
    - sletning af nøgler, når de ikke længere skal bruges
    - monitorere og revision af nøglehåndteringsaktiviteter
    - fastsætte aktiverings- og deaktiveringsdatoer for nøgler, så nøglerne kun kan bruges i det tidsrum, der er fastsat i enhedens regler for nøglehåndtering
    - håndtere juridiske anmodninger fra retsinstanser om adgang til kryptografiske nøgler.

Dokumentation

Alle relevante medarbejdere i enheden bør have adgang til politikker og procedurer for brug af kryptografi og kryptering i enheden.

Politikken og procedurerne for kryptografi bør gennemgås med planlagte intervaller samt ved erkendte sårbarheder eller teknologiske fremskridt, der kan påvirke sikkerheden i den anvendte kryptografi. Det kan eksempelvis være en algoritme, der bliver brudt, eller at behovet for nøglelængde øges som følge af øget computerkraft hos angribere.

Hvis en gennemgang af politikker eller procedurer afdækker sårbarheder, skal dokumentationen og de tekniske løsninger opdateres, og ændringerne skal kommunikeres til relevante parter.

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.5.31, A.8.24
NIST CSF 2.0
PR.AA-01, PR.DS-01, PR.DS-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04
IEC 62443
IEC 62443-3-3:2013 SR 1.8, SR 1.9, SR 3.1. RE 1, SR 4.1, SR 4.3
EECC
SO13
ETSI EN 319 401
Clause 7.5, ref. til afsnit 10 i ISO/IEC 27002:2013

EKSEMPEL PÅ RELEVANTE OVERVEJELSER OM KRYPTOGRAFI I EN OMFATTET ENHED (1/2)

En virksomhed er omfattet af NIS 2-loven, da den leverer kritiske transportydelser. Virksomheden har både it- og OT-systemer, samt mange leverandører – herunder cloud- og serviceudbydere. Nedenfor nævnes en række centrale overvejelser vedrørende virksomhedens kryptografi.

Beskyttelse af forsyningsdata og kommunikation med leverandører

- Er kommunikationen med leverandører (f.eks. cloud, ERP, logistiksystemer) end-to-end krypteret?
- Anvendes VPN-forbindelser og sikre API'er med opdaterede protokoller (TLS 1.3+)?
- Er integritet og autenticitet af leverandørdata (f.eks. produktionsparametre, opdateringspakker) valideret kryptografisk?
- Kan leverandører dokumentere, at de anvender kryptering, der lever op til virksomhedens krav?
- Er kryptografiske krav en del af leverandøraftaler og sikkerheds-forpligtelser (SLA/DPA)?
- Er der tilsyn og audit af leverandørers nøglehåndtering og krypteringspraksis?

Kryptering af data i systemer

- Er sensitive data, der behandles eller lagres, krypteret i hvile og i transit?
- Beskytter virksomheden kommunikation mellem PLC'er, sensorer og SCADA-systemer med egnet kryptering, hvor det er muligt?
- Er det sikret, at eksterne leverandører ikke kan manipulere med firmware eller produktionsdata via usikre forbindelser?

Sikker nøglehåndtering

- Har virksomheden en centraliseret nøglehåndteringsløsning (f.eks. HSM, KMS) til håndtering af nøgler på tværs af OT og it?
- Er der styr på nøglerotation og tilbagekaldelse, hvis en leverandør kompromitteres?
- Hvordan håndteres nøgler til cloud-leverandører og underleverandører?

EKSEMPEL FORTSAT (2/2)

Overvågning og hændelseshåndtering

- Har virksomheden logning og alarmering for fejl i kryptografiske processer (f.eks. nøglefejl, certifikatproblemer)?
- Er der beredskabsprocedurer for kompromitterede nøgler, særligt i forhold til leverandørkommunikation?

Teknologisk vedligehold og trusselsudvikling

- Følger vi udviklingen i kryptografisk sikkerhed (f.eks. PQC – post-quantum cryptography)?
- Er der processer for opgradering af krypteringsalgoritmer og nøglelængder, når det teknologiske stade ændres?

9. PERSONALESIKKERHED, ADGANGSKONTROLPOLITIKKER OG FORVALTNING AF AKTIVER

Det siger NIS 2-loven:

§ 6, stk. 1, nr. 9 *Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.*

Lovbemærkninger
Det foreslås i nr. 9, at foranstaltninger skal omfatte eller tage højde for personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.

Dette indebærer bl.a., at enhederne skal implementere foranstaltninger til personalesikkerhed, der skal sikre, at den enkelte medarbejder forstår, udviser og forpligter sig til at leve op til deres ansvar for informationssikkerhed.

Enheder skal derudover udarbejde en politik for adgangskontrol for at beskytte mod uautoriseret adgang til enhedens net- og informationssystemer. Politikken skal som minimum identificere og vurdere risici i forhold til logisk og fysisk adgangskontrol og indeholde procedurer for styring af adgangsrettigheder.

Enheder skal fastlægge, hvordan den forvalter aktiver, der vil kunne påvirke sikkerheden i enhedens omfattede net- og informationssystemer.

A. PERSONALESIKKERHED

Formål

At sikre, at ansatte, samarbejdspartnere, og hvor relevant leverandører, forstår og forpligter sig til deres sikkerhedsansvar i overensstemmelse med enhedens politik for informationssystemsikkerhed.

Foranstaltning

Enheden skal sikre, at medarbejdere og – hvor relevant – leverandører eller tjenesteudbydere er bekendt med og lever op til deres ansvar for enhedens net- og informationssystemssikkerhed. Dette skal ske i forhold til de tjenester, enheden udbyder, og i overensstemmelse med enhedens politik for informationssystemsikkerhed[29].

[29] Se "1.a. Politik for informationssystemssikkerhed"

Enheden kan udarbejde procedurer til at sikre at:

- alle ansatte, direkte leverandører og tjenesteudbydere, hvor det er relevant, er bekendt med og følger den standardpraksis for cyberhygiejne, som enheden anvender[30]
- alle brugere med administrativ eller privilegeret adgang er bekendt med og handler i overensstemmelse med deres roller, ansvarsområder og bemyndigelser
- at medlemmer af ledelsesorganer forstår og handler i overensstemmelse med deres rolle, ansvarsområder og bemyndigelser med hensyn til sikkerheden i net- og informationssystemer (for mere information se vejledning om ledelsens rolle og opgaver).

Sikkerhedsansvar kan skrives ind i kontrakter og ansættelsesaftaler.

Enheden kan udføre baggrundskontrol af nyansatte og, hvor det er relevant, af direkte leverandører og konsulenter, hvis det er påkrævet ud fra en risikovurdering af deres rolle, ansvar, beføjelser, og de net- og informationssystemer, som de får adgang til. Baggrundskontrol kan være alt fra kontrol af eksamensbeviser, jobreferencer, personers identitet (f.eks. ved fremvisning af billedelegitimation), validering af certificering, til sikkerhedsgodkendelser i offentligt regi.

Hvis det vurderes relevant at udføre baggrundskontrol, bør enheden:

- indføre kriterier for de roller, ansvarsområder og bemyndigelser, der kun må udøves eller indehaves af personer, hvis baggrund er blevet kontrolleret
- sikre, at kontrollerne tager hensyn til gældende love, forskrifter og etiske regler
- sikre, at der foretages baggrundskontrol af disse personer, inden de begynder at udøve disse roller og bemyndigelser eller tildeles disse ansvarsområder.

Enheden bør sikre, at ansvar og pligter for net- og informationssikkerhed, der stadig er gyldige efter afslutning af ansættelsesforholdet eller ændring i ansættelsen, er defineret, kommunikeret og forstået.

Enheden bør udarbejde og kommunikere de ansættelsesretslige regler, der gælder i tilfælde af overtrædelser af politikker og procedurer koblet til sikkerheden i net- og informationssystemer.

Dokumentation

Enheden kan sikre sig, at der i medarbejdernes ansættelsesaftaler anføres, at medarbejderen er forpligtet til at gennemføre den nødvendige uddannelse og træning i den net- og informations-sikkerhed enheden definerer, samt at medarbejderen er bekendt med deres ansvar for at efterleve enhedens politikker og procedurer for net- og informationssikkerhed. Medarbejderens nærmeste leder bør godkende medarbejderes kompetencer og retskaffenhed.

Dokumentation kan være i form af nedskrevne politikker og procedurer for, hvordan enheden eksempelvis gennemfører baggrundskontrol og aftrædelsessamtaler. Politikker og procedurer bør gennemgås med passende planlagte mellemrum.

[30] Se "7. Cyberhygiejne og cybersikkerhedsuddannelse"

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.5.28, A.6.1, A.6.2, A.6.3 A.6.4, A.6.5, A.6.7, A.7.1, A.7.2
NIST CSF 2.0
PR.AT-2, GV-RR-04, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04
IEC 62443
IEC 62443-2-1: 2010 4.3.3.2, 4.3.3.2.2, 4.3.3.2.3, IEC 62443-2-4: 2015 SP 01.04, SP 01.07
EECC
SO5, SO6, SO7, SO8
ETSI EN 319 401
REQ-7.2, REQ-7.2-10, REQ-7.2-05

B. ADGANGSKONTROL

Formål

At beskytte fysiske og ikke fysiske aktiver imod tab af fortrolighed, integritet og tilgængelighed ved at beskytte dem mod uautoriseret adgang.

Foranstaltning

Enheden skal udarbejde en politik for at administrere tildeling, ændring og fjernelse af adgangs-rettigheder til net- og informationssystemer i overensstemmelse med enhedens politik for informationssystemsikkerhed[31].

Politikken skal som minimum identificere og vurdere risici i forhold til logisk og fysisk adgangskontrol (eksempelvis adgang til digitale systemer og bygninger). Det dækker både personers og processers adgang til net- og informationssystemer. Eksempelvis når et eksternt net- og informationssystem skal forbindes til et internt system.

[31] Se "1.a. Politik for informationssystemsikkerhed"

Politikken skal indeholde procedurer for styring af adgangsrettigheder, herunder administration af privilegerede adgangsrettigheder. Procedurerne bør omfatte:

- metoder til at identificere og vurdere medarbejderes, leverandørers og serviceudbyderes behov for tildeling af rettigheder og adgange for både almindelige brugere og brugere med udvidede administratorrettigheder
- metoder til løbende at sikre at medarbejderes, leverandørers og serviceudbyderes adgangsrettigheder tildeles, ændres eller fjernes efter behov.

Enheden bør begrænse og kontrollere brugen af it-administrationssystemer og systemer, der kan ændre i sikkerhedskonfigurationen i it-komponenter. Politikken kan omhandle både adgange for medarbejdere og eksterne, såsom leverandører af varer, tjenester mv.

Enheden bør styre og dokumentere identiteter for brugere og systemer, der har adgang til enhedens informationer og relaterede aktiver. Enheden bør sikre sig og dokumentere, hvilke personer eller systemer der har adgang til dens net- og informationssystemer, og hvorfor de har adgang. Styringen bør omfatte identifikation, ændring, revurdering og afvisning af identitet for brugere og systemer. Enheden bør implementere sikre autentificeringsprocedurer og -teknologier på baggrund af adgangskontrolpolitikken[32].

Dokumentation

Dokumentation kan være i form af nedskrevne politikker og procedurer vedrørende tildeling af, ændring i og fratagelse af adgang til enhedens lokaler og net- og informationssystemer. Politikker og procedurer bør gennemgås med passende planlagte mellemrum.

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.5.3, A.5.15, A.5.16, A.5.17, A.5.18, A.7.2, A.8.2, A.8.3, A.8.5, A.8.18, A.8.21, A9
NIST CSF 2.0
PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04
IEC 62443
IEC 62443-2-1:2010 4.3.3.5, 4.3.3.5.4, 4.3.3.6, 4.3.3.6.3, 4.3.3.7 IEC 62443-3-3:2013 SR 1.3, SR 2.1, SR 2.2
EECC
SO11
ETSI EN 319 401
REQ-7.4-04A, REQ-7.4-05, REQ-7.4-06, REQ-7.4-07, REQ-7.4-08, REQ-7.4-10

[32] Se bl.a. ”10.a. Multifaktorautentificering”

C. FORVALTNING AF AKTIVER

Formål

At sikre en passende beskyttelse af det enkelte aktiv eller typer af aktiver. Forvaltning af aktiver sikrer, at enheden får indsigt i hvilke aktiver, enheden skal beskytte, og hvilket beskyttelsesniveau der er passende for de enkelte aktiver.

Foranstaltning

Enheden skal fastlægge, hvordan enheden forvalter aktiver, der vil kunne påvirke enhedens net- og informationssikkerhed. Enheden bør derfor udarbejde procedurer for forvaltning af alle enhedens aktiver, herunder net- og informationssystemer, tilhørende komponenter samt kritiske afhængigheder mellem disse og eventuelle samarbejdspartnere. Der bør defineres et passende beskyttelsesniveau for de aktiver, der er omfattet af enhedens net- og informationssystemer. Eksempelvis har mobile enheder ofte et andet beskyttelsesbehov end stationære servere.

Enheden:

- bør udarbejde en procedure til at fastsætte relevante klassifikationsniveauer for aktiver med henblik på det krævede beskyttelsesniveau for alle aktiver, herunder informationer der er omfattet af enhedens net- og informationssystemer. Beskyttelsesniveauerne bør fastsættes i forhold til aktivernes følsomhed, kritiske betydning, risiko og forretningsværdi
- bør udarbejde og kommunikere instruktioner for korrekt håndtering af aktiver, i overensstemmelse med politikken for informationssystemsikkerhed[33] i hele deres livscyklus - ved anskaffelse, brug, opbevaring, transport og bortskaffelse. I den bør indgå regler, der beskytter data ved brugen af flytbare medier
- kan udvikle og vedligeholde en fortegnelse over net- og informationssystemer og tilhørende aktiver. Enheden bør i den forbindelse sikre, at denne fortegnelse forbliver komplet, nøjagtig og retvisende. Ændringer i fortegnelsen dokumenteres, så det er muligt at konstatere, hvad der er ændret. Dette bør i givet fald indgå i enhedens ændringsstyring
- bør stille krav om, at alle interne og eksterne medarbejdere returnerer eller uigenkaldeligt sletter de aktiver, som de har fået udleveret, så snart ansættelses- eller kontraktforholdet ophører.

Dokumentation

Dokumentation kan være i form af nedskrevne procedurer vedrørende håndtering af aktiver, samt dokumentation for, hvordan disse kommunikeres til relevante parter. Procedurerne bør gennemgås med planlagte intervaller.

[33] Se "1.a Politik for informationssystemssikkerhed"

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.5.9, A.5.10, A.5.11, A.5.12, A 5.13, A.5.14, A.5.18, A.7.7, A.7.10, A.8.24
NIST CSF 2.0
PR.DS-01, ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05, ID.AM-07, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04
IEC 62443
IEC 62443-2-1:2010 4.3.3.2, 4.2.3.4, 4.2.3.6, 4.3.4.4.2, 4.3.4.4.3, 4.3.4.4.6, A.2.3.3.8.3, IEC 62443-3-3:2013 SR 2.3, SR 2.4, SR 7.8
EECC
SO04, SO07, SO17
ETSI EN 319 401
REQ-7.3, REQ-7.3.1-02, REQ-7.3.2

10. MULTIFAKTORAUTENTIFICERING OG NØDKOMMUNIKATIONSSYSTEMER

Det siger NIS 2-loven:

§ 6, stk. 1, nr. 10 *Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikations-systemer internt hos enheden, hvor det er relevant.*

Lovbemærkninger

Det foreslås med nr. 10, at foranstaltninger skal omfatte eller tage højde for brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nød-kommunikationssystemer internt hos enheden, hvor det er relevant.

Dette indebærer bl.a., at enheder skal anvende multifaktorautentifikation eller kontinuerlig autentifikation ved adgang til net- og informationssystemer i overensstemmelse med enhedens politik for adgangskontrol. Enheder skal endvidere anvende sikret tale-, video- og tekstkommunikation i overensstemmelse med politikken for brug af kryptografi og kryptering og under hensyntagen til kommunikationsmidlernes tilgængelighed, også i en nødsituation.

A. MULTIFAKTORAUTENTIFICERING

Formål

At styrke adgangskontrollen og reducere risikoen for uautoriseret adgang ved at kombinere flere autentifikationsfaktorer og løbende vurdere adfærd og kontekst.

Foranstaltning

Enhedens brugere, it-komponenter og andre aktiver skal, hvor det vurderes relevant, autentificeres ved hjælp af multifaktorautentifikation (MFA) og/eller kontinuerlige autentifikations-mekanismer ved adgang til enhedens net- og informationssystemer. Autentifikationskravene bør fastlægges med udgangspunkt i en risikovurdering og matche aktivets klassifikationsniveau (ud fra fortrolighed, integritet og tilgængelighed). Autentifikationen skal være i overensstemmelse med enhedens adgangskontrolpolitikker[34].

[34] Se "9.a. Adgangskontrol".

MFA bør (med udgangspunkt i risikovurderingen) anvendes, når man tilgår:

- aktiver ved fjernadgang
- administrative systemer
- følsomme informationer eller fortrolige data (f.eks. personoplysninger[35] eller forretningskritiske informationer)
- systemer med høj værdi for enheden eller med stor konsekvens ved kompromittering.

Enheden kan ud fra aktivets klassifikation vurdere, om det eksempelvis skal være på netværksniveau, systemniveau eller dokumentniveau.

MFA kan eksempelvis bestå af minimum to af følgende faktorer:

- noget brugeren ved (f.eks. password eller PIN)
- noget brugeren har (f.eks. en token, engangskode eller sikkerhedsnøgle)
- noget brugeren er (f.eks. biometriske data som fingeraftryk eller ansigtsgenkendelse).

Kontinuerlig autentifikation kan anvendes til løbende at monitorere og verificere en brugers eller et systems identitet under en aktiv session ved hjælp af adfærds- og kontekstuelle faktorer. Det kan eksempelvis være ved adgangsforsøg:

- fra ukendt lokalition
- fra en ukendt eller nyregistreret enhed
- på et usædvanligt tidspunkt eller i afvigende mønstre.

Enhedens brug af kontinuerlig autentifikation kan være koblet til enhedens processer og værktøjer til monitorering[36].

MFA kan kombineres med kontinuerlig autentifikation, så yderligere faktorer (f.eks. brug af token eller risikovurdering af aktiviteten) kræves baseret på foruddefinerede regler eller ændringer i brugerens adfærd og sessionens kontekst, såsom mistænkelig aktivitet.

Dokumentation

Enheden skal med regelmæssige planlagte mellemrum, eller ved større ændringer og sikkerheds-hændelser, gennemgå politikken for adgangskontrol[37] og i den forbindelse gennemgå og vurdere enhedens brug af MFA og/eller kontinuerlig autentifikation. Gennemgangen skal dokumenteres.

[35] Vær opmærksom på databeskyttelseskrav i databeskyttelsesloven.
[36] Se "2.b. Logning og monitorering"
[37] Se "9.a. Adgangskontrol"

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.5.17, A.8.5
NIST CSF 2.0
PR.AA-03, PR.AA-05, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04
IEC 62443
IEC 62443-2-1:2010 4.3.3.6, 4.3.3.6.3, IEC 62443-3-3:2013 SR 1.1. RE 1, SR 1.1 RE 2, SR 1.1 RE3, SR 1.2, SR 1.5, SR 1.6, SR 1.7
EECC
SO11
ETSI EN 319 401
REQ-7.4-08

B. NØDKOMMUNIKATIONSSYSTEMER

Formål

At sikre, at enheden altid har mulighed for at anvende tale-, video- og tekstkommunikation, hvor og når det er relevant, herunder i tilfælde af hændelser. Kommunikationskanalerne skal sikre den nødvendige fortrolighed, integritet og tilgængelighed internt hos enheden.

Foranstaltning

Enheden bør vurdere deres behov for kommunikationskanaler, inklusiv enhedens behov for at beskytte fortrolighed ved brug af kryptering eller behov for redundante kommunikationsløsninger. Disse kommunikationsløsninger bør også indgå i enhedens risikovurdering samt i enhedens procedurer for driftskontinuitet, hændelseshåndtering og krisestyring[38]. Der bør fastlægges foranstaltninger på grundlag heraf.

Enheden kan eksempelvis:

- udarbejde planer for sikker kommunikation i tilfælde af en væsentlig hændelse – planerne kan indeholde eskaleringsprocedure samt intern og ekstern rapportering til samarbejdspartnere, sektoransvarlige myndigheder og CSIRT[39]
- beskrive eksterne og interne kommunikationskanaler, samt hvordan de hver især aktiveres og anvendes samt evt. genetableres i tilfælde af nedbrud
- sikre tilgængelighed af kommunikationskanaler ved at etablere en passende redundans, således at der altid er alternative kanaler til rådighed[40]

[38] Se "1.b. Politik for risikostyring", "2.a. Håndtering af hændelser","3.c. Redundans", "3.d. Krisestyring" og "8. Kryptografi"
[39] Se "2.a. Håndtering af hændelser" og "3.d. Krisestyring"
[40] Se "3.c. Redundans"

- etablere krisestyringsprocesser, der indeholder passende kommunikationsmuligheder mellem enheden og deres eventuelle sikkerhedstjenester, de relevante sektoransvarlige myndigheder, CSIRT'en og andre relevante interessenter
- etablere muligheden for kommunikation mellem forskellige systemer gennem pålidelige kanaler, der er isoleret ved hjælp af logisk, kryptografisk eller fysisk adskillelse fra andre kommunikationskanaler og beskytter datastrømme mod ændring eller offentliggørelse.

Tale-, video- og tekstkommunikationskanaler kan f.eks. være alternative VoIP-løsninger, krypterede beskedtjenester, VHF-radioer, SINE-telefoner, satellittelefoner eller SMS. Valgte kanaler bør understøtte fortrolighed (f.eks. via kryptering) og være tilgængelige uafhængigt af enhedens primære systemer. Det bør være aftalt, hvilket klassifikationsniveau man må kommunikere på via kommunikationskanalerne.

Dokumentation

Nødkommunikationssystemer bør testes regelmæssigt og kan indgå som en del af en årlig krisestyringsøvelse[41]. Resultatet af tests og øvelserne bør dokumenteres for at sikre, at der samles op på de fejl, man finder, og den læring øvelserne tilvejebringer.

Internationale standarder og rammeværk

DS/EN ISO/IEC 27001:2023
A.5.30, A.5.31, A.7.8, A.7.12, A.8.14, A.8.20, A.8.22 m.fl.
NIST CSF 2.0
GV.OC-04, PR.AT-01, PR.AT-02, RS.CO-02, RS.CO-03, RS.MA-01. RS.MA-04
IEC 62443
-
EECC
-
ETSI EN 319 401
-

[41] Se "3.d Krisestyring"

ANDRE RELEVANTE MATERIALER (1/2)

Nedenfor fremgår en række vejlednings- og kommunikationsmaterialer, som kan være relevante i forhold til implementering af cybersikkerhedsforanstaltninger.

Materialet er til inspiration og er ikke udviklet med henblik på at opfylde specifikke lovkrav.

Sikkerdigital.dk
På sikkerdigital.dk kan virksomheder og myndigheder finde viden, vejledning og konkrete værktøjer til deres arbejde med cyber- og informationssikkerhed.

Trusselsvurderinger fra SAMSIK
SAMSIK udgiver løbende sektorspecifikke trusselsvurderinger, som enheder kan bruge i deres risikostyring. Derudover udgiver SAMSIK emnespecifikke trusselsvurderinger, samt den nationale trusselsvurdering "Cybertruslen mod Danmark" og "Nationalt Risikobillede".

Vejledning om grundlæggende cyberforsvar
Vejledningen "Cyberforsvar der virker" er en grundlæggende vejledning om cyberforsvar og håndtering af cyberangreb.
Vejledningen er tilgængelig på samsik.dk/cybervejledninger.

Vejledning om cybersikkerhed i leverandørforhold
Vejledningen "Cybersikkerhed i leverandørforhold" giver gode råd til, hvordan man kan oprette og bibeholde et godt samarbejde mellem kunden og leverandøren af it-driften, gennem hele samarbejdsperioden. Fra valg af leverandør til ophør af samarbejdet.
Vejledningen er tilgængelig på samsik.dk/cybervejledninger og sikkerdigital.dk.

Vejledning om logning
Vejledningen " Logning – en del af et godt cyberforsvar" giver gode råd til, hvor i netværket man skal logge, og hvad man bør logge. Den bygger på erfaringer fra bl.a. it-sikkerhedsfirmaer i forbindelse med bistand ved hændelseshåndtering.
Vejledningen er tilgængelig på samsik.dk/cybervejledninger.

ANDRE RELEVANTE MATERIALER (2/2)

Vejledning om password-sikkerhed
Vejledningen beskriver nogle af de angrebsmetoder, som hackere benytter sig af, samt nogle af de eksisterende udfordringer ved passwords. Vejledningen indeholder desuden en række konkrete anbefalinger til, hvordan man – på forskellige niveauer i en organisation – bør arbejde med password-sikkerhed.
Vejledningen er tilgængelig på samsik.dk/cybervejledninger.

Vejledning om at imødegå ransomware-angreb
Vejledningen "Reducér risikoen for ransomware" giver en række anbefalinger, som organisationer kan følge for at reducere sandsynligheden for at blive ramt af ransomware-angreb. Vejledningen giver desuden råd til, hvordan et ransomware-angreb kan håndteres, når skaden er sket.
Vejledningen er tilgængelig på samsik.dk/cybervejledninger.

Vejledning om at imødegå phishing-angreb
Vejledningen "Beskyt din organisation mod phishing-angreb" hjælper organisationer med at imødegå truslen fra phishing-mails.
Vejledningen er tilgængelig på samsik.dk/cybervejledninger.

Vejledning om beskyttelse mod DDoS-angreb
Vejledningen "Beskyt mod DDoS-angreb" kommer med en række forholdsregler, som en organisation kan tage for at beskytte sig mod DDoS-angreb.
Vejledningen er tilgængelig på samsik.dk/cybervejledninger.

Vejledning om IoT-enheder
Vejledningen " Beskyt IoT-enheder" kommer med konkrete anbefalinger til, hvordan organisationer kan beskytte IoT-enheder efter best practice.
Vejledningen er tilgængelig på samsik.dk/cybervejledninger.

Vejledning om adfærdsindsatser
Vejledningen "Metode til at arbejde med adfærdsindsatser inden for cyber- og informationssikkerhed" giver indsigt i, hvordan man kan arbejde med adfærdsindsatser, der kan styrke cyber- og informationssikkerheden i en organisation.
Vejledningen er tilgængelig på samsik.dk/cybervejledninger og sikkerdigital.dk.