NOTAT

Dato: 26-06-2025
Kontor: KCIS

Vejledning til Indberetning af sikkerhedshændelse efter NIS2-direktivet

Overblik

Blanketten er delt op i følgende elementer:

1. Kontaktoplysninger mm.
2. Valg af indberetning og sektor
3. Hændelsesforløbet
4. omfang
5. Tidslinje
6. Øvrige involverede
7. Håndtering
8. Opsummering og indsendelse

Særlige bemærkninger

Blanketten er dynamisk, så alt efter hvilke felter du udfylder, kan det åbne for andre og supplerende spørgsmål.

Sektorer: Du kan vælge flere typer indberetning og flere sektorer, og så vil blanketten blive sendt til flere myndigheder samtidig, alt efter dine valg.

Sidst i dokumentet finder du en samlet oversigt over spørgsmålene i blanketten.

Proces

Når du indsender blanketten, bliver den sendt til Erhvervsstyrelsen, som automatisk sender videre til de relevante myndigheder, baseret på dine valg af sektorer. Hermed har du færdiggjort registreringen.

Hvis det bliver aktuelt, vil du høre direkte fra myndighederne.

Husk at downloade en kopi af blanketten, når du har sendt den. Kopien er dit bevis på, at du har sendt en indberetning.

Yderligere hjælp

- Faglige spørgsmål:
  - kontakt den myndighed, du ønsker at indberette til. Du finder et samlet overblik her.

- Hjælp med Virk.dk eller adgang til blanketten:
  - Vejledning: https://virk.dk/vejledning/virk-hjaelp/
  - Virk support: Ring 72 20 00 30

Hændelsesindberetning efter NIS2 – oversigt over spørgsmål

NB: alt efter valg i blanketten kan der være supplerende spørgsmål

Identifikation

Identifikation af sikkerhedshændelsen

- Er dette en uddybning af en tidligere anmeldelse?

Oplysninger om indberetter

- CVR
- Myndighedens/virksomhedens navn
- Afdeling
- Adresse
- Kontaktperson (navn og titel)
- E-mail på kontaktperson
- Telefonnummer på kontaktperson
- Internt referencenummer

Indberetning på en andens vegne

- Indberetter du på en andens vegne? (Eksempelvis den dataansvarlige)

Hvad vedrører hændelsen

- Hændelse vedrørende den finansielle sektor (DORA)
- Brud på persondatasikkerheden (GDPR)
- Hændelse vedrørende samfundskritisk infrastruktur eller digitale tjenester (NIS2-direktivet) (både lovpligtige og frivillige underretninger)
- Frivillig indberetning af hændelser i øvrige sektorer til Forsvarets Efterretningstjeneste (CSIRT)
- Indberetning vedrørende eIDAS forordningen
- Indberetning efter CER direktivet (Energistyrelsen)

Sektor

- Hvilken sektor tilhører indberetter?
- Hvilken enhedstype tilhører indberetter?

Valgte myndigheder

Ud fra ovenstående valg vil din indberetning blive sendt til følgende: (dannes automatisk)

Væsentlig hændelse eller frivillig underretning

- Angiv om underretning er en lovpligtig underretning af en væsentlig hændelse, eller om det er en frivillig underretning

Hvilken indberetning er der tale om

- 24 timers underretning (tidlig varsling)
- 72 timers underretning (ajourføring af tidlig varsling)
- Endelig rapport

Hændelsesforløbet og relevante årsager

- Sigende titel
- Beskriv hændelsesforløbet
- Mulighed for at uploade vedhæftninger (.pdf)
- Er det en tilbagevendende hændelse?
- Er indberetningen af denne hændelse relevant for, eller forbundet til, en anden hændelse?
- Type af sikkerhedsbrud
- Angiv type af hændelsen
    - Menneskelige fejl
    - Systemfejl
    - Procesfejl
    - ondsindede handlinger
    - Naturfænomener
    - Tredjepartsfejl

    (uddybes efterfølgende yderligere)

Type af hændelse

- Udfald (tilgængelighed og/eller service kontinuitet er påvirket)
- Anden påvirkning af service (fortrolighed, autenticitet eller integritet er påvirket)
- Påvirkning af andre systemer
- Påvirkning af redundans

Hvilke funktionelle områder og forretningsprocesser blev påvirket?

Omfang

Størrelse af hændelsens påvirkning. Hvor stor påvirkning har hændelsen haft?

- Ingen påvirkning
- Mindre påvirkning
- Stor påvirkning
- Meget stor påvirkning

- Angiv hvor mange personer, der har været berørt af hændelsen
- Øvrige oplysninger om omfanget
- Hvilke systemer er omfattet af hændelsen?

Påvirket teknisk udstyr

- Hæveautomater eller kasseapparater
- Arbejdsstationer
- Switche eller routere
- Industrielle systemer
- Website
- E-mailkonto
- Servere eller domain controllers
- Applikation eller app
- Mobilbasestationer eller controllere Systemer til fysisk sikring af f.eks. bygninger Nødstrømsanlæg inkl. UPS.
- Nedgravede kabler
- Undersøiske kabler
- Andet

- Angiv funktionsområder og forretningsprocesser, der er påvirket af hændelsen, herunder produkter og tjenester

Kompromitteringsindikatorer

- IP-adresser
- URL'er
- Domæner
- E-mailadresser (fx ved phishing)
- Hashværdier (fx malware, scripts eller vedhæftede filer)
- Certifikater (fx SSL-certifikater)
- Tilgængelige logfiler (fx serverlogs, domain controller, klienter)
- Andet
- Ved ikke

- Beskriv typen af information eller tilgængelige oplysninger i fritekstfeltet nedenfor

Information omkring udnyttet sårbarhed

- Egen vurdering af kritikaliteten for ikke kendte sårbarheder
    - Lav
    - Medium
    - Høj
    - Kritisk

Geografisk område

- Har trafik til et eller flere andre lande end Danmark ikke været mulig?

- Har mere end 50% af kapaciteten hos en udbyder af offentligt tilgængelige elektroniske kommunikationsnet og tjenester på en ikke brofast ø med mere end 1.500 individer været berørt?

Grænseoverskridende hændelser

- Påvirker hændelsen/kan hændelsen påvirke personer i andre EU- eller EØS-lande?
- Vurderes hændelsen at have væsentlige konsekvenser for tjenester i andre EU- eller EØS- lande?

Påvirkning og faktorer

Tværsektoriel påvirkning.

- Påvirker hændelsen andre sektorer?
    - Påvirker ikke andre sektorer
    - Påvirker alle sektorer

Påvirker specifikke sektorer

Faktorer for betydning af udfaldet.

- Væsentligste faktorer i samlet vurdering af hændelsens betydning.
    - Antal brugere
    - Procentdel af berørte brugere
    - Udfaldets varighed
    - Geografisk spredning
    - Økonomisk tab
    - Immateriel skade
    - Andet

Tidslinje

Dato og tidspunkt for hændelsens konstatering

- Hvordan blev hændelsen konstateret på dette tidspunkt?
- Angiv sammenlagt varighed af hændelsen (husk at angive enhed: Timer, dage / uger / måneder)
- Varighed af udfald i tjeneste

Øvrige involverede i hændelsen (databehandlere, underleverandører, mv.)

- Er der involveret eksterne samarbejdspartnere? (databehandlere, underleverandører el. lignende)

Håndtering

- Er du i dialog med den kompetente myndighed vedrørende beredskab/krisestyring?
- Har du behov for teknisk assistance til håndteringen fra Forsvarets Efterretningstjeneste (CSIRT)?
- Er hændelsen anmeldt til politiet?

Foranstaltninger af teknisk og organisatorisk karakter, der er truffet på baggrund af hændelsen

- Beskriv tekniske og organisatoriske foranstaltninger gennemført for at stoppe hændelsen
- Beskriv tekniske og organisatoriske foranstaltninger gennemført efter at hændelsen er blevet stoppet
- Beskriv tekniske og organisatoriske foranstaltninger som skal gennemføres efter hændelsen for at forhindre, at det gentager sig i fremtiden
- Hvad har I gjort af erfaringer i forbindelse med hændelsen? (lessons learned)