Nasjonal kommunikasjons-myndighet

Varsling og rapportering av sikkerhetshendelser innen tillitstjenester

Varslingsregimet omtalt her gjelder kun de forpliktelser tilbydere av tillitstjenester har overfor Nkom.

Tidlig varsling til myndighetene om alvorlige hendelser innen tillitstjenester anses som svært viktig. Nasjonal kommunikasjonsmyndighet (Nkom) skal varsles så raskt som mulig etter at en hendelse har skjedd og senest 24 timer etter tilbyder har blitt oppmerksom på hendelsen. Dette er for å kunne koordinere tiltak samt styre informasjonsflyten mellom de som er involvert i og omfattet av hendelsen samt ivareta de plikter som er omfattet av det europeiske samarbeidet innen tillitstjenester. Varsler er også viktig for å kunne identifisere trender og kampanjer innen trusler og hendelser som omfatter sektoren.

Hjemmelsgrunnlaget for å kreve at en tilbyder varsler myndighetene finnes i forordning om eID og tillitstjenester (eIDAS)-forordningen) eIDAS artikkel 19 nr. 2:

> *2. Kvalifiserte og ikke-kvalifiserte tilbydere av tillitstjenester skal så snart som mulig og senest 24 timer etter å ha fått kjennskap til sikkerhetsbrudd eller tap av integritet som i betydelig grad påvirker tillitstjenesten eller personopplysninger som oppbevares i forbindelse med levering av tjenesten, underrette tilsynsorganet og eventuelt andre berørte organer, for eksempel vedkommende nasjonale organ for informasjonssikkerhet eller personvernmyndighet.*
>
> *Dersom det er trolig at et sikkerhetsbrudd eller tap av integritet vil ha negativ innvirkning på en fysisk eller juridisk person som har benyttet seg av tillitstjenesten, skal tilbyderen av tillitstjenesten så snart som mulig også underrette den fysiske eller juridiske personen om sikkerhetsbruddet eller tapet av integritet.*
>
> *Når det er relevant, særlig dersom et sikkerhetsbrudd eller tap av integritet gjelder to eller flere medlemsstater, skal det meldte tilsynsorganet underrette tilsynsorganene i andre berørte medlemsstater samt ENISA.*

Nasjonal kommunikasjonsmyndighet
Besøksadresse:
Nygård 1, Lillesand

Postadresse:
Postboks 93
4791 LILLESAND

Tel: 22 82 46 00
Fax: 22 82 46 40
firmapost@nkom.no

NO 974 446 871
www.nkom.no

Det meldte tilsynsorganet skal underrette offentligheten eller kreve at tilbyderen av tillitstjenestene gjør dette, dersom det fastslår at det er i offentlighetens interesse at sikkerhetsbruddet eller tapet av integritet offentliggjøres.

Definisjoner

Tillitstjeneste:
eIDAS-forordning artikkel 3 nr. 16

16) «tillitstjeneste» en elektronisk tjeneste som normalt tilbys mot betaling, og som består av

a) framstilling, kontroll og validering av elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler, elektroniske tjenester for registrert sending og sertifikater knyttet til slike tjenester eller

b) framstilling, kontroll og validering av sertifikater for nettstedsautentisering eller

c) bevaring av elektroniske signaturer, segl eller sertifikater knyttet til slike tjenester,

Sikkerhetshendelse:
Ethvert sikkerhetsbrudd, tap av integritet eller tilgjengelighet som påvirker tillitstjenesten eller personopplysninger som oppbevares i forbindelse med leveranse av tillitstjenesten. En «all-hazard» tilnærming blir brukt, hvor enhver hendelse som kan tenkes å påvirke tillitstjenesten eller personopplysninger, blir klassifisert som en sikkerhetshendelse.

Nasjonal kommunikasjons-myndighet

Varsling

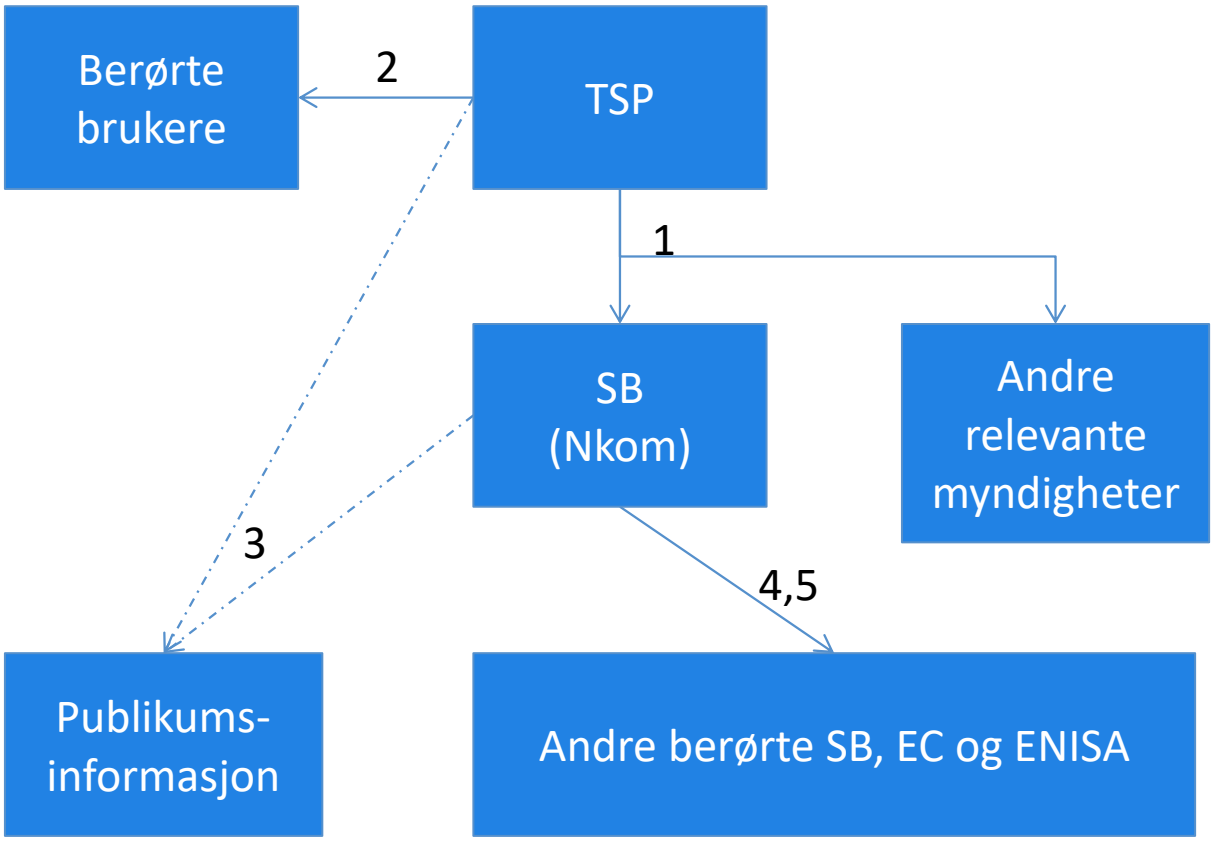
Nkom har beredskapsvakt 24/7 som vil motta og vurdere alle varsler som sendes inn av tilbydere av tillitstjenester. Ut fra en helhetsvurdering av situasjonen vil Nkom enten ta varslet til orientering, eller starte en videre oppfølgning av hendelsen.

Nkom vil ta kontakt med en oppgitt kontaktperson hos tilbyder dersom vi ser behov for å følge opp hendelsen underveis, eller dersom det i etterkant ønskes en hendelsesrapport.

Rapporteringsstruktur

Oppfølgning av sikkerhetshendelsen følger en rapporteringsstruktur hvor det avhengig av hendelsen vil være nødvendig å følge opp en eller flere av punktene nedenfor.

1. Tilbyder av tillitstjeneste er pliktig å varsle om en sikkerhetshendelse så snart som mulig og maksimalt 24 timer etter at hendelsen er blitt oppdaget. Andre varslingsplikter må også overholdes.
2. Tilbyder av tillitstjenester er pliktig å informere, uten unødvendig opphold, alle naturlige eller juridiske personer som er negativt berørte av hendelsen
3. Publikum kan tenkes å måtte bli informert dersom hendelsen vurderes til å være av offentlig interesse. Nødvendighet vurderes av tillitstjenestetilbyder, men kan også bli pålagt av Nkom.
4. Nkom vil om nødvendig varsle andre relevante nasjonale tilsynsorgan for tillitstjenester dersom hendelsen berører mer enn en europeisk nasjon.
5. Nkom vil årlig rapportere sikkerhetshendelser til ENISA og Europakommisjonen.



Hvem skal varsle?
Alle tilbydere av tillitstjenester er pliktige å varsle om sikkerhetshendelser.

Når skal Nkom varsles?
Nkom skal varsles så raskt som mulig etter at en sikkerhetshendelse har skjedd og senest 24 timer etter tilbyder har blitt oppmerksom på hendelsen.

Hvilke sikkerhetshendelser skal varsles?
Alle sikkerhetshendelser som tilbyder av tillitstjenester vurderer til å ha betydelig påvirkning på tillitstjenester eller personopplysninger. Tilbydere av tillitstjenester skal rapportere sikkerhetshendelser som omfatter systemer eller prosesser som er under tilbyderens kontroll. I de tilfeller hvor kjernefunksjonalitet blir ivaretatt av en tredjepart er tilbyderen av tillitstjenesten ansvarlig for å varsle om sikkerhetshendelser som forekommer i tredjeparts systemer eller prosedyrer.

For å vurdere hvorvidt en sikkerhetshendelse har betydelig påvirkning på tillitstjenester eller personopplysninger brukes skalaen som er vist i tabellen nedenfor. Sikkerhetshendelser som er av alvorlighetsgrad 3 eller høyere skal varsles.

Alvorlighetsgrad og omfang
1. Ingen påvirkning
2. Ubetydelig påvirkning: tilbyders ressurser er berørt men ingen påvirkning på tjenestene
3. Betydelig påvirkning: mindre andel av kunder/tjenester er berørt
4. Stor påvirkning: stor andel av kunder/tjenester er berørt
5. Katastrofe: hele organisasjonen og alle kunder/tjenester er berørt

En sikkerhetshendelse som kun omfatter en enkelt kunde skal i utgangspunktet ikke varsles. Unntakene for dette er som følger:

- Dersom det oppstår et større antall enkelthendelser med utspring i, eller som kan relateres til samme årsak.
- Dersom sikkerhetshendelsen avdekker en sårbarhet som potensielt kan føre til at et større antall kunder kan bli berørt.
- Dersom hendelsen omfatter kunder med samfunnskritiske funksjoner eller andre tilbyderes tjenester.

Hva skal et varsel til Nkom om en sikkerhetshendelse inneholde?

- Når hendelsen oppstod
- Når hendelsen ble oppdaget
- Navn på tillitstjenestetilbyder som er rammet
- Kontaktperson hos tilbyder (telefon og epost)
- Kortfattet beskrivelse av tillitstjenester som er rammet
- Beskrivelse av eventuell persondata som er berørt
- Kortfattet beskrivelse av hendelsen
- Kortfattet beskrivelse av omfang
- Kortfattet beskrivelse av årsak
- Varighet før hendelsen forventet mitigiert
- Mottiltak som er foretatt eller planlagt iverksatt
- En indikasjon på hvorvidt utenlandske kunder er berørt

Hvordan skal det varsles?

Tilbyder av en tillitstjeneste skal logge seg inn på Altinn og hente ut skjema for varsling til Nkom av en sikkerhetshendelse for tillitstjenester. Skjema skal fylles ut og sendes inn. Nkom får da varsel på epost om innsendt skjema. Det er også mulig å kontakte Nkoms beredskapsvakt på 22 33 17 00 dersom det er spørsmål til rapporteringen.

Nasjonal kommunikasjons-myndighet

Hendelsesrapportering

Nkom kan kreve utfyllende hendelsesrapporter etter en sikkerhetshendelse. Nkom kan også kreve hendelsesrapporter der tilbyder selv ikke vurderte at varsling var nødvendig.

Mal for hendelsesrapport

Tidslinje for hendelsen

- Hvor skjedde hendelsen
- Tidspunkt hendelsen startet
- Tidspunkt hendelsen ble oppdaget
- Tidspunkt hendelsen ble normalisert
- Rapporteringstider til eventuelt berørte brukere, publikum andre relevante aktører

Beskrivelse av hendelsen og foranledning/årsak

- Generell beskrivelse av sikkerhetshendelsen
    - Kort beskrivelse av tillitstjenester som var involvert
    - Beskrivelse av hendelsen
        - Komponenter involvert og var det eventuelt brudd på konfidensialitet, integritet eller tilgjengelighet
- Hva var årsak til hendelsen
    - Rot årsak: menneskelig feil, ondsinnet handling, systemfeil, naturkatastrofe
    - Detaljert årsak
- Hvordan ble hendelsen oppdaget

Omfang av hendelsen

- Antall berørte brukere
    - Absolutt og andel av total
    - Eventuelle åpenbart samfunnsviktige kunder berørt (eks. sykehus o.l.)
- Berørte hendelsen brukere/kunder i andre europeiske nasjoner
    - Inkluderer ikke norske borgere som oppholder seg i utlandet
- Kostnadsestimat

Skadereduserende tiltak

- Beskrivelse av eventuelle tiltak iverksatt for å forhindre/redusere skadekonsekvensene etter at sikkerhetshendelsen var detektert.

Skadeforebyggende tiltak

- Beskrivelse av eventuelle tiltak iverksatt for å forhindre/redusere denne type hendelse fra å inntreffe på nytt.

Eksempler på alvorlighetsgrad og omfang

Eksempler på nivå 2

- Forsinkelser i produksjon av signatur/segl når plattformen genererer alle signaturer.
- Forsinkelser i validering av signatur når plattform validerer alle signaturer.
- Volumavhengig:
  - En kunde prøver å få sertifikat på falsk grunnlag (ikke samfunnsviktige funksjoner).
  - Et smartkort blir forsvinner eller blir stjålet.

Eksempler på nivå 3

- Signeringstjeneste er nede.
- Valideringstjeneste er nede.
- Utfall av tilgjengelighet av tillitstjenester
- Gammel CRL tillater bruk av tilbaketrukne sertifikat

Eksempler på nivå 4

- Inkonsistens mellom OCSP og CRL
- Feil eller manglende oppdateringer genererer fører til at signaturplattform genererer signaturer som ikke kan valideres.

Eksempler på nivå 5

- Kompromittering av nøkkelenheter: For eksempel HSM, eller smartkort, USB tokens, FIDO tokens.