Nasjonal sikkerhetsmyndighet (NSM)

Rundskriv 1/11

Rapportering av sikkerhetstruende hendelser til NSM

1 Bakgrunn og hensikt

Dette rundskrivet omhandler sikkerhetstruende hendelser som virksomheter underlagt sikkerhetsloven plikter å rapportere til Nasjonal sikkerhetsmyndighet (NSM), samt former for rapportering.

"Nasjonal sikkerhetsmyndighet skal innhente og vurdere informasjon av betydning for gjennomføringen av forebyggende sikkerhetstjeneste." Dette følger av sikkerhetsloven § 9. Videre slår § 5 fast: "Enhver virksomhet plikter å utøve forebyggende sikkerhetstjeneste i henhold til bestemmelsene gitt i eller i medhold av loven her." Avslutningsvis følger det av § 5: "Nærmere bestemmelser gis av Nasjonal sikkerhetsmyndighet."

Forskrift om sikkerhetsadministrasjon er gitt i medhold av sikkerhetsloven og regulerer "Reaksjon ved sikkerhetstruende hendelser" i kapittel 5. Dette rundskrivet er såkalte "nærmere bestemmelser" gitt av NSM, som referert til ovenfor i sikkerhetsloven. Disse bestemmelsene er dermed gitt i medhold av loven og NSM har derfor en forventning om at de følges på linje med bestemmelsene i forskriften.

Det er viktig å sikre at informasjon om sikkerhetstruende hendelser som skjer i eller oppdages av virksomheter, og som kan ha betydning for rikets sikkerhet, vitale interesser eller selvstendighet, blir registrert og rapportert til NSM. Rapportering av sikkerhetstruende hendelser til NSM bidrar blant annet til å:

a) sikre at virksomheten kan dra nytte av NSM sin rådgivning for best mulig håndtering av enkelthendelser
b) avdekke trender og sammenhenger som det kan være vanskelig å se for den enkelte virksomhet, og dermed
c) sikre et korrekt og rettidig bilde av rikets sikkerhetstilstand og risikonivå
d) gi grunnlag for risikoanalyser
e) gi mulighet til snarest mulig å iverksette forebyggende sikkerhetstiltak iht. risikobildet
f) sikre at sikkerhetsavtaler med andre nasjoner og internasjonale organisasjoner blir opprettholdt[1]
g) gi NSM muligheten å fungere som en felles informasjonssentral hvis mange virksomheter blir rammet av en hendelse samtidig.

2 Virksomhetens ansvar og plikter

2.1 Plikt til å utøve forebyggende sikkerhetstjeneste etter sikkerhetsloven § 5

Hovedansvaret påhviler lederen for virksomheten. I tillegg har alt ansatt og engasjert personell i sitt arbeid eller oppdrag for virksomheten ansvar for å ivareta sikkerhetsmessige hensyn, og plikter å bidra til forebyggende sikkerhetstjeneste.

2.2 Plikt til å rapportere uønskede og sikkerhetstruende hendelser

Forskrift om sikkerhetsadministrasjon og Veiledning i sikkerhetsadministrasjon omhandler virksomheters plikt til å rapportere uønskede hendelser til NSM:

I Forskrift om sikkerhetsadministrasjon, § 5-6. Rapportering til NSM, heter det*:*
"En virksomhet skal snarest mulig avgi foreløpig rapport til NSM dersom den oppdager sikkerhetstruende hendelser eller sikkerhetsbrudd vedrørende informasjon sikkerhetsgradert av utenlandske myndigheter eller internasjonale organisasjoner."

Denne bestemmelsen er i brev fra Forsvarsdepartementet, om Rapportering til Nasjonal sikkerhetsmyndighet (datert 20. november 2007), definert til å bety: En virksomhet skal snarest mulig avgi foreløpig rapport til NSM dersom den oppdager: "a) sikkerhetstruende hendelser, eller b) sikkerhetsbrudd vedrørende informasjon sikkerhetsgradert av utenlandske myndigheter eller internasjonal organisasjon".

I Veiledningen i sikkerhetsadministrasjon, § 6.3 Håndtering av uønskede hendelser, heter det:
" Uønskede hendelser må rapporteres og registreres internt i virksomheten." Videre følger det at *"alle sikkerhetstruende hendelser må rapporteres til NSM."*

3 Hva rapporteres til NSM?

I Tabell 1 følger er en oversikt med overordne kategorier av, samt definisjoner og eksempler på, selvforskyldte, observerte eller mulige sikkerhetstruende hendelser som virksomheter underlagt sikkerhetsloven plikter å rapportere til NSM.

TABELL 1 – RAPPORTERINGSPLIKTIGE SIKKERHETSTRUENDE HENDELSER[2]

Sikkerhetstruende hendelser	**Definisjon**	**Eksempler -** noen av mange mulige rapporteringspliktige sikkerhetstruende hendelser
1) Sikkerhetstruende virksomhet *(bevisste handlinger)*	Forberedelse til, (forsøk på) gjennomføring av, og medvirkning til spionasje, sabotasje eller terrorhandlinger	- Uvedkommende viser spesiell interesse for anlegg og installasjoner, personer, eller skjermingsverdig(e) informasjon/objekter/aktiviteter - Planlegging/gjennomføring av angrep mot vitale nasjonale IKT-systemer og/eller kritisk infrastruktur - Bevisst ulovlig utveksling av skjermingsverdig informasjon mellom norske og utenlandske personer/organisasjoner, med hensikt å misbruke denne - Bevisst lekkasje/salg av skjermingsverdig informasjon (f. eks til media) - Gjennomføring og/eller mistanke om ulovlig avlytting av, eller innsyn i, rom som er permanent sikret mot teknisk avlytting eller innsyn
2) Kompromittering av skjermingsverdig informasjon *(ubevisste handlinger)*	Tap eller mistanke om tap av konfidensialitet, integritet eller tilgjengelighet for skjermingsverdig informasjon – herunder uønsket avhending, modifisering eller ødeleggelse	- Skjermingsverdig informasjon kommuniseres og/eller lagres på ugradert system - Mistanke om kompromittering av skjermingsverdig informasjon fremkommet under tekniske undersøkelser - Brudd på bestemmelser for rom som er permanent sikret mot teknisk avlytting eller innsyn - HEMMELIG / STRENGT HEMMELIG informasjon omtales eller feilbehandles/ -oppbevares utenfor sperret område - Sikkerhetsbrudd ved nødrett og nødverge[3]
	Sikkerhetstruende hendelser rettet mot kryptosikkerhet	- Tap eller feilhåndtering/-lagring av kryptonøkler eller annet kryptoutstyr - Feil eller mangelfull rapportering av kryptoregnskap (skal håndteres iht. Forskrift om informasjonssikkerhet §§ 7-41 – 7-45[4]).
3) Grove sikkerhets-brudd	Sikkerhetsbrudd som har medvirket, eller det er uvisst om har medvirket til sikkerhetstruende virksomhet eller kompromittering	- En ulåst kontor-, hvelv- eller safedør til/i sperret område - Bruk av feil, eller ufullstendig, fysisk sikring (ikke-godkjent låsetype til sperret område, etc.) - Bruk av minnepinne med skjermingsverdig informasjon, eller som det *har* vært slik informasjon på, på ugradert system - Skjermingsverdig informasjon kommer bort eller behandles uforsvarlig utenfor beskyttet/sperret område - Manglende oversikt på hvem i virksomheten som har håndtert og/eller hatt

		tilgang til skjermingsverdig informasjon - Hendelse/brudd som virksomheten selv anser som alvorlig eller kritisk
	Sikkerhetsbrudd som innebærer at flere sikkerhetsbarrierer er gjennombrutt eller som skyldes systematiske feil i virksomhetens forebyggende sikkerhetstjeneste	- Gjentagende forekomst av: ulåst dør/skap, personell tar med nøkkel hjem, glemt å slå av PC eller lignende til/i kontrollert/beskyttet område - Permanent dårlig fysisk sikring av skjermingsverdig informasjon/objekt - Gjentatte brudd på virksomhetens interne sikkerhetsrutiner/-prosedyrer
4) Sikkerhetsbrudd – internasjonalt gradert informasjon	Sikkerhetsbrudd relatert til mulig/faktisk kompromittering av skjermingsverdig informasjon/objekt gradert av utenlandsk myndighet eller internasjonal organisasjon[5]	- Sikkerhetstruende hendelser definert og omtalt i punkt 1), 2), og 3), som omfatter informasjon/utstyr/systemer gradert av utenlandsk myndighet eller internasjonal organisasjon, inkludert; - Uaktsom oppbevaring/fordeling/håndtering av skjermingsverdig utenlandsk informasjon, som kan medføre tap, eller mistanke om tap, av konfidensialitet, tilgjengelighet eller integritet for informasjonen, som f. eks. at et: - ikke-NATO-medlem, eller uautorisert personell, gis/får/har tilgang til NATO-gradert informasjon - NATO-gradert dokument blir feilaktig omgradert til norsk gradering, o.l.

Ved sikkerhetstruende hendelse må sikkerhetsansvarlig og ledelsen i virksomheten vurdere å orientere politiet eller om forholdet skal anmeldes. NSM må underrettes om politianmeldelse gjennomføres.[6]

4 Form for rapportering til NSM

Ved sikkerhetstruende hendelse skal sikkerhetsansvarlig i virksomheten straks avgi foreløpig rapport til NSM. Rapportering til NSM skal primært foregå på minst én av følgende måter:

4.1 Elektronisk hendelsesrapporteringsskjema – kun UGRADERT INNHOLD

NSM har et selvforklarende elektronisk hendelsesrapporteringsskjema tilgjengelig på sin nettside. Dette skjemaet kan **IKKE innholde spesifikk gradert informasjon** om hendelsen, men likevel hentyde til type og alvorlighetsgrad av hendelsen og eventuelt fungere som et varsel om at en mer detaljert rapport blir oversendt/-levert senere – da iht. graderings- og forsendelsesprosedyre beskrevet i 4.2 under. Sikkerhetsansvarlig eller leder i virksomheten skal verdivurdere informasjonen og sørge for at innholdet i rapporten er ugradert før rapporteringsskjema oversendes elektronisk.

4.2 Hendelsesrapporteringsskjema – utskriftsversjon

Dersom virksomheten, ved sikkerhetsansvarlig, vurderer den elektroniske måten å rapportere på som uegnet, som for eksempel ved at gradert informasjon må/bør inkluderes, skriv ut og fyll inn rapporteringsskjema for sikkerhetstruende hendelse, tilgjengelig på NSM sin nettside. Dersom virksomheten vurderer informasjonen i hendelsesrapporten som[7]:

1. Ugradert / Unntatt offentlighet / FORTROLIG / BESKYTTET eller BEGRENSET
   a. send skjema som ordinær post, eller
   b. lever personlig
2. STRENGT FORTROLIG / KONFIDENSIELT eller HEMMELIG
   a. send skjema i dobbel emballasje, enten som registrert postsending eller med kurer, eller
   b. ta personlig kontakt med NSM
3. STRENGT HEMMELIG
   a. send skjema i dobbel emballasje med kurer, eller
   b. ta personlig kontakt med NSM[8]

4.3 Andre rapporteringsformer til NSM

Ved alvorlige hastesaker, eller om de ovennevnte former anses som uegnet, rapporter snarest til NSM på en eller flere av følgende måter:

- **Ugradert** telefon: 67 86 40 00 / 02497
- **Ugradert** e-post: post@nsm.stat.no
- **Ugradert** telefaks: 67 86 40 09
- Gradert e-post: Kan brukes av personell med tilgang til gradert system (ring NSM for nærmere opplysninger)
- Gradert telefaks: Kan brukes av personell med tilgang til gradert system (ring NSM for nærmere opplysninger)
- Personlig overlevering / Kurer: Kolsås leir – Rødskiferveien 20, Kolsås, Bærum

4.4 Mulighet for anonymitet

Så fremt det er mulig ønsker NSM at virksomhet som oppdager, eller er kilden til, en sikkerhetstruende hendelse oppgir virksomhetsnavn og navnet på kilden til hendelsen ved rapportering til NSM. Virksomheter kan likevel – når dette anses formålstjenlig – velge å holde kilden til, eller rapportøren av hendelsen anonym. NSM ser det som viktigere at hendelser blir registrert, rapportert, håndtert og analysert på en rask og hensiktsmessig måte, enn at rapportøren og/eller kilden blir gjort kjent for NSM.

4.5 Andre rapporteringshensyn

- Dersom rapporten inneholder personopplysninger, må disse skjermes i henhold til krav i personopplysningsloven
- Skulle ny, viktig informasjon i saken fremkomme etter førstegangsrapportering, skal en utfyllende rapport fremsendes snarest
- Endelig rapport med sammenfatning av alle opplysninger og undersøkelser, og med informasjon om gjennomførte og planlagte tiltak, fremsendes når saken anses avsluttet
- Rapporter kan slås sammen når saken avsluttes kort tid etter at hendelsen eller bruddet ble oppdaget
- Ved kompromittering av informasjon sikkerhetsgradert KONFIDENSIELT eller høyere må virksomheter informere tilvirker av informasjonen. Tilvirker må deretter gjøre en skadevurdering, som rapporterende virksomhet så oversender en kopi av til NSM.

5 Hendelsesrapporteringsblankett for intern bruk – papirblokkversjon

NSM oppfordrer enhver ansatt i virksomhet underlagt sikkerhetsloven om å ha en hendelsesrapporteringsblankett lett tilgjengelig for bruk ved intern rapportering av uønskede sikkerhetshendelser.[9] En blokk med slike kan bestilles ved å kontakte NSM, eller ved å fylle ut bestillingsskjema på NSM sin nettside.

6 Konklusjon

Rapportering av sikkerhetstruende hendelser er primært ”hjelp til selvhjelp”, ved at både virksomheten og samfunnet potensielt blir sikrere. Den bidrar til effektiv håndtering av enkelthendelser, så vel som til nyttige analyser og derved bedre forebyggende sikkerhetsarbeid og -tiltak. Anse derfor innrapportering av observerte eller selvutførte, bevisste eller ubevisste sikkerhetstruende hendelser som en positiv og samfunnsnyttig handling.

Husk at innrapportering av sikkerhetstruende hendelser til NSM er en lovpålagt plikt.

---

[1] Ved kompromittering av gradert informasjon som omfattes av internasjonale avtaler plikter Norge, ved NSM, å rapportere slike iht. Sikkerhetsavtale med NATO C-M(2002)49.

[2] Informasjonen i Tabell 1 er primært hentet fra følgende (del)dokumenter:
Sikkerhetsloven § 3, nr. 2 – sikkerhetstruende virksomhet definert;
Forskrift om sikkerhetsadministrasjon § 1-2, nr. 2 – 4 – om sikkerhetstruende hendelse, kompromittering og sikkerhetsbrudd;
Forskrift om sikkerhetsadministrasjon § 2-2 – om rapportering av manglende skikkethet;
Forskrift om sikkerhetsadministrasjon § 2-3, 2. ledd, nr. 5 og 6 – om personellets rapportering;
Forskrift om sikkerhetsadministrasjon § 5-3 – om nødrett og nødverge;
Forskrift om sikkerhetsadministrasjon § 5-4 – om rapportering og registrering av sikkerhetstruende hendelser.
Ytterligere bestemmelser er gitt i Forskrift om informasjonssikkerhet.

[3] Straffelovens § 47 og 48 om nødrett og nødverge er et negativt uttrykt ansvarsvilkår i strafferetten: Den som handler i en nødsituasjon etter bestemmelsene opptrer så vel rettmessig som straffefritt.

[4] For rapporteringsprosedyre, se også Vedlegg U til veiledning for administrativ kryptosikkerhet: ”Rapport om sikkerhetstruende hendelse” (Ref. Forskrift om informasjonssikkerhet § 7-41 til 7-45). Tilgjengelig på www.nsm.stat.no.

[5] Se Sikkerhetsavtale med NATO C-M(2002)49.

[6] Forskrift om sikkerhetsadministrasjon § 5-7 – om rapportering til politiet.

[7] Se Forskrift om informasjonssikkerhet § 4-20 om emballering. Dette gjelder både nasjonalt graderingsnivå og tilsvarende internasjonalt graderingsnivå.

[8] Se Forskrift om informasjonssikkerhet § 4-19 – om forsendelsesmetode.

[9] Se Veiledning om interne rapporteringsrutiner ved uønskede hendelser. Tilgjengelig på www.nsm.stat.no.