Riktlinjer för säkerhet i telenät och teletjänster

Bilaga 3: Integritetsincidenter

Ver. 1.1

TLP:CLEAR

STADSNÄTS FÖRENINGEN

INNEHÅLSFÖRTECKNING

1 Inledning

Detta dokument utgör ett förslag till utformning av en Process för ett stadsnäts Integritetshantering. Anvisningen beskriver processen för hanteringen av en integritetsincident eller vid en uppenbar risk för att en integritetsincident kan inträffa.

Processen baseras på ITIL Incident Management och tillämpliga delar av Problem Management med beaktande av nedanstående krav:

PTSFS 2022:11, Kap. 13 § 1: Kräver att alla incidenter rapporteras internt.
PTSFS 2022:11, Kap. 17 § 1: Kräver att alla säkerhetsincidenter rapporteras.
CSL/NIS2: Kräver att incidenter rapporteras inom 24 timmar.

Lag (2006:544): Föreskriver åtgärder vid extraordinära händelser och incidenter.

2 Syfte

Processen ska säkerställa att alla integritetsincidenter identifieras, hanteras, dokumenteras och rapporteras internt, till berörda parter och relevanta myndigheter på ett strukturerat sätt för att minimera påverkan och förbättra den övergripande säkerheten.

3 Begrepp och definitioner

Integritetsincident: en händelse där personuppgifter eller annan känslig information som hanteras av operatören exponeras, förloras, ändras, raderas, eller på annat sätt behandlas på ett otillbörligt sätt. Detta kan innefatta både avsiktliga och oavsiktliga handlingar som bryter mot dataskyddslagar eller interna säkerhetspolicyer, och som kan leda till intrång i kundernas personliga integritet.

4 Roller och ansvarsfördelning

I detta avsnitt används begreppet (företagsspecifik) för att ange att rollen/funktionen är beroende av hur företaget väljer att organisera verksamheten.

Informationssäkerhetschef (företagsspecifik)

Informationssäkerhetschefen har det övergripande ansvaret för hanteringen av integritetsincidenter och ansvarar för att:

- Ta emot integritetsincidenter
- Utse incidentansvarig
- Följa upp genomförandet av åtgärder för en integritetsincident
- Utveckla och förvalta processen genom att planlägga och genomföra:
    - regelbundna översyner
    - identifiering av förbättrings- och anpassningsbehov
    - ledning och koordinering av arbetet med förbättringar och anpassning i samråd med Processägaren.
    - Dokumentera, publicera och kommunicera processen.
    - Utveckla och förvalta ärendehanteringsverktygen.
    - Bedöma bemanningsbehov för processen.
    - Genomföra uppföljningsmöten för granskning av hanteringen av incidenter.
    - Utbilda medarbetare i supportorganisationen kring arbetet i ärendehanteringsprocessen

Incidentansvarig

Person som tilldelats ansvaret för leda arbetet med att hantera en integritetsincident.

- Koordinera och driva arbetet vid incidenter.
- Säkerställa att alla berörda parter får relevant information. Informationen till kunderna prioriteras.
- Incidenter rapporteras enligt gällande föreskrifter.

Åtgärdsfunktion

Funktion som tilldelats ansvaret för att utarbeta och implementera lösningar för att åtgärda och skadebegränsa en integritetsincident.

5 Tillämpning

Förtydligande av aktiviteter i integritetsprocessen

Se Bilaga 1, Process för integritetsincidenter.

5.1 Tar emot incident

Anmälan om en integritetsincident kan komma in på olika sätt till exempel via anställda, externa parter, en supportfunktion eller via systemövervakning. Ärendet ska överlämnas till Informationssäkerhetschefen eller av denne utpekad incidentansvarig inom organisationen vilket kan vara ett dataskyddsombud (om ett sådant finns) eller annan ansvarig för säkerhetsfrågor.
Incidentansvarig kontrollerar om ärendet är pågående, kontrollerar status och informerar anmälaren om så är fallet.

Incidentlogg

Vid integritetsincidenter ska den som tillhandahåller en kommunikationstjänst löpande föra en förteckning/incidentlogg i enlighet med 8 kap. 9 § lagen (2022:482) om elektronisk kommunikation. Incidentloggen ska innehålla nedanstående uppgifter och kompletteras under processen:

- 1. datum då integritetsincidenten inträffade,
- 2. en beskrivning av integritetsincidenten,
- 3. uppskattat antal berörda abonnenter eller användare,
- 4. bedömda konsekvenser av integritetsincidenten,
- 5. orsak till att integritetsincidenten inträffade,
- 6. de åtgärder som vidtagits, och
- 7. referensnummer.

Incidentloggen kompletteras succesivt under ärendets process.
Ansvarig. Incidentansvarig.

5.2 Klassificerar och bedömer

Bedöm omfattningen av incidenten. Här avgörs vilken typ av personuppgifter som är påverkade, hur allvarlig händelsen är, och vilka konsekvenser det kan få för de individer vars data har exponerats eller påverkats.

Initial incidentrapportering

Ärendet rapporteras till interna intressenter i enlighet med *Rutin för intern incidentrapportering*.

Kontrollerar om det krävs rapportering till myndigheter. Vid behov rapportera enligt gällande föreskrifter och enligt *Rutin för extern incidentrapportering*.

5.3 Utvärderar, riskbedömer och tilldelar

Här görs en bedömning av vad som kan ha orsakat incidenten och om den inträffade incidenten innebär en hög risk för de enskilda individernas rättigheter och friheter. Detta kan till exempel handla om att deras integritet eller säkerhet är i fara, exempelvis genom identitetsstöld.

Om incidenten bedöms innebära en hög risk för de berörda individerna måste de informeras omedelbart. Informationen ska vara tydlig och ge vägledning om vad de kan göra för att skydda sig, exempelvis genom att ändra lösenord eller vara vaksamma på bedrägeriförsök.

5.4 Åtgärdar och skadebegränsar

En fördjupad analys av incidenten och bakomliggande orsaker genomförs. Det ska göras en kontroll av om det finns tidigare beskrivna incidenter och deras lösningar eller om det finns information om kända fel eller information om workaround.
Åtgärder för skadebegränsning ska identifieras och prioriteras.

Utarbetar lösning, implementerar och dokumenterar lösningen

En lösning utarbetas och implementeras. Lösningen och implementeringen testas för att verifiera att lösningen är korrekt.

5.5 Dokumentera, klarrapportera och stäng ärendet

Dokumenterar

Incidentloggen uppdateras och de åtgärder som genomförts för att lösa incidenten dokumenteras för att kunna ge viktig information när nya incidenter kommer in. Detta bidrar till att man då snabbt kan lösa dem. Uppdatera dokumentationen.

Klarrapporterar

Ärendet klarrapporteras till Informationssäkerhetschefen (företagsspecifik) och interna intressenter.

Avslutat ärendet

Ärenden stängs av den funktion som har ansvarat för ärendet. Vid kundinitierade ärenden stämmer åtgärdsfunktionen av med kunden att det är ok att stänga ärende.

6 Integritetsrapporter

6.1 Till Myndighet

Att alla inträffade säkerhetsincidenter dokumenteras och rapporteras till relevanta myndigheter så som Integritetsskyddsmyndigheten (IMY) och Post och telestyrelsen (PTS).

- **IMY rapportering:** använd IMY checklista vid personuppgiftsincidenter. Rapport ska lämnas inom 72 timmar.
- **PTS rapportering:** Organisationen ska rapportera integritetsincidenter i enlighet med 8 kap. 8 § lagen (SFS 2022:482, LEK) om elektronisk kommunikation och kommissionens förordning (EU) nr 611/2013. Rapporterna ska lämnas till PTS inom specificerad tid från det att incidenten upptäcktes.

6.2 Till berörda verksamheter och individer

Efter avslutat ärende lämnas en Integritetsrapport till berörda verksamheter och individer.

Rutin för rapportering av säkerhetsincidenter.

Ansvarig för incidentrapportering är incidentansvarig.

7 Uppföljningsmöte

Efter att incidenten hanterats bör organisationen analysera vad som gick fel och varför. Åtgärder bör vidtas för att förhindra att något liknande inträffar igen, till exempel genom att förbättra säkerhetssystem eller utbilda personal.

8 Underlag till andra processer

Rapportering till processer som påverkats av incidenterna samt för kontinuitets- och kvalitetsuppföljning.