KIESRAAD

Werkproces

Onderwerp
Incidentmeldingen

Opgesteld door: 5.1.2.e
Eigenaar: 5.1.2.e

Versiebeheer

Versie	Datum	Auteur(s)	Opmerkingen
0.1	Maart 2023	5.1.2.e	Eerste concept
1.0	3 april 2023	5.1.2.e	Vastgesteld en goedgekeurd door DO-B

Introductie

Dit document omschrijft het werkproces van zowel de kant van de melder als van de behandelaar van informatiebeveiligingsincidentmeldingen (in dit document verder aangeduid als "incidentmelding(en)".

Het proces gaat nadrukkelijk **niet** over het inhoudelijk afhandelen van incidenten. Dit is een proces dat interdisciplinair dient te worden afgestemd en geformuleerd.

De doelgroep van dit document is iedereen binnen de Kiesraad die geïnteresseerd is in het incidentmeldproces, de verantwoordelijke behandelaar(s), de CISO en de plv. secretaris directeur.

Terminologie[1]

Term	Omschrijving
Behandelaar	De medewerker die de melding in behandeling neemt.
Chief Information Security Officer (CISO)	Medewerker die verantwoordelijk is voor de processen rondom informatiebeveiliging binnen de Kiesraad.

[1] Alle hier gebruikte termen zijn tevens opgenomen in de algemene begrippenlijst van de Kiesraad en dienen te worden geüpdate bij wijzigingen. De schuingedrukte tekst geeft uitleg die alleen relevant is voor dit document en daarom niet in de begrippenlijst staat.

Datalek	Het onbedoeld of ongeautoriseerd beschikbaar komen van informatie. Zowel met als zonder dat er sprake is van persoonsgegevens.
Datalek conform AVG	Het onbedoeld of ongeautoriseerd beschikbaar komen van informatie die conform de Algemene Verordening Gegevensbescherming een persoonsgegeven zijn.
Incidentafhandelingsproces	Nog te ontwikkelen proces om alle soorten incidenten af te handelen. *Het verschilt met dit proces in dat het tevens niet gemelde incidenten betreft. Daarnaast beschrijft het hoe incidenten dienen te worden afgehandeld, waar het proces in dit document omschrijft hoe de afhandeling van meldingen dient te verlopen.*
Incidentenregister	Excelbestand waarin alle incidenten zijn opgenomen met korte omschrijving en relevante kenmerken. Met dit register worden analyses en rapportages gemaakt.
Informatie	Alle vormen van data/gegevens zowel gesproken, geschreven, digitaal of fysiek, als anderszins welke in hun context enige betekenis hebben.
Informatiebeveiligingsincident (incident)	Een gebeurtenis die de beschikbaarheid, integriteit en/of vertrouwelijkheid van informatie van de Kiesraad in gevaar brengt of dreigt te brengen.
Melder	Iemand die een incident meldt.
Ticket	Een digitale plek waar registratie van gebeurtenissen, incidenten, aanvragen, gesprekken etc kunnen worden gemaakt. Hierbij is het mogelijk bestanden, screenshots en andere details toe te voegen om het mogelijk te maken om achteraf te volgen hoe een afhandelingsproces is verlopen.
Ticketsysteem	Software waarin het mogelijk is om tickets aan te maken. Bijvoorbeeld TopDesk of JIRA.

Korte omschrijving proces

Het doel van dit proces is het zo correct mogelijk afhandelen van incidenten op een (achteraf) controleerbare manier, zonder de identiteit van de melder onnodig bekend te maken binnen de organisatie.

De Kiesraad moet een plek hebben waar medewerkers en externen (vermoedens van) incidenten kunnen melden. Deze moeten vervolgens worden opgepakt en beoordeeld door iemand met kennis van informatiebeveiliging en privacy. Zonder dit proces kunnen incidenten burgers, de Staat, externe organisaties en de Kiesraad zelf potentieel (ernstige) schade toebrengen. Het proces heeft als doel te zorgen voor een traceerbaar onderdeel van het incident afhandelingsproces. Het is onderdeel van het nog te omschrijven incident afhandelingsproces.

Workflow

1. Melder merkt een (mogelijk) incident op.
2. Melder stuurt email met informatie over incident naar 5.1.2.i@kiesraad.nl.
3. Behandelaar ontvangt email en leest deze.
4. Behandelaar maakt een ticket aan in het ticketsysteem. Zet daarin de inhoudt van de email inclusief de contactgegevens van de melder en eventuele bijlagen/screenshots etc.
5. Behandelaar bevestigd aan de melder dat de melding is ontvangen en in behandeling zal worden genomen.
6. Behandelaar onderzoekt de melding en vraagt eventueel om aanvullende informatie bij de melder.
7. Behandelaar registreert alle onderzoekshandelingen en aanvullende informatie in het aangemaakte ticket.
8. Behandelaar neemt eventueel maatregelen conform het incidentafhandelingsproces. En registreert deze handelingen in het aangemaakte ticket.
9. Behandelaar informeert alle betrokkenen dat de melding de status afgehandeld zal krijgen en sluit het ticket.
10. Behandelaar sluit het ticket en registreert het incident in het incidentenregister.

Toelichting

Hieronder staat per stap uit de flow uitgelegd hoe deze dient te worden uitgevoerd.

1. Melder merkt een (mogelijk) incident op

Het kan hier gaan om een email (met persoonsgegevens) die is verzonden naar een verkeerde ontvanger. Een gestolen laptop of verloren notitieboek met aantekeningen waarin vertrouwelijke informatie staat etc.

Het kan ook gaan om een incident waar de melder zelf niet (direct) bij betrokken is. Bijvoorbeeld dat een melder ziet dat een medewerker een toegangspas is verloren.

De melder kan zowel een medewerker van de Kiesraad zijn als een leverancier of iemand van buiten de organisatie.

2. **Melder stuur email met informatie over incident naar** 5.1.2.e **@kiesraad.nl**

Ook wanneer een melder telefonisch of mondeling een melding maakt in de eerste instantie, verzoeken wij de melder het alsnog ook per email te melden. Dit maakt het proces transparanter en kan misverstanden achteraf over wat de melder precies heeft willen melden voorkomen. Alleen in zeer uitzonderlijke gevallen kan een melder volledig anoniem blijven bij een melding. Dit dient de CISO[2] naar eigen inzicht te beoordelen en motiveren achteraf.

3. **Behandelaar ontvangt email en leest deze.**

De CISO dient er zorg voor te dragen dat alle emails die naar 5.1.2.i @kiesraad.nl worden verzonden binnen 72 uur in behandeling worden genomen door een behandelaar. Dit, in verband met de regelgeving uit de AVG en de mogelijke ernst van incidenten.

4. **Behandelaar maakt een ticket aan in het ticketsysteem. Zet daarin de inhoudt van de email inclusief de contactgegevens van de melder en eventuele bijlagen/screenshots etc.**

Door een ticket aan te maken is een centrale plaats ontstaan waar alle relevante informatie kan worden bewaard en later kan worden teruggezien en gecontroleerd of is gehandeld conform de afgesproken procedures.

5. **Behandelaar bevestigd aan de melder dat de melding is ontvangen en in behandeling zal worden genomen.**

De melder moet weten dat de melding is ontvangen. Soms zijn melders in paniek of emotioneel door een incident. Door de ontvangst te bevestigen kan dit wellicht deels worden weggenomen. Iemand gaat helpen.

6. **Behandelaar onderzoekt de melding en vraagt eventueel om aanvullende informatie bij de melder.**

Dit zal plaatsvinden conform het nog te formuleren incidentafhandelingsproces.

7. **Behandelaar registreert alle onderzoekshandelingen en aanvullende informatie in het aangemaakte ticket.**

Dit is nodig voor transparantie en controleerbaarheid.

8. **Behandelaar neemt eventueel maatregelen conform het incidentafhandelingsproces. En registreert deze handelingen in het aangemaakte ticket.**

Dit zal plaatsvinden conform het nog te formuleren incidentafhandelingsproces

9. **Behandelaar informeert alle betrokkenen dat de melding de status afgehandeld zal krijgen en sluit het ticket.**

Wanneer alle handelingen en maatregelen die noodzakelijk zijn conform de geldende afspraken en procedures zijn uitgevoerd en verder geen relevante acties open staan kan het incident worden gezien als afgehandeld. Soms denkt een behandelaar dat alle mogelijke acties zijn uitgevoerd, maar heeft een van de betrokkenen daar een ander perspectief op. Daarom is het goed betrokkenen te

---

[2] De behandelaar kan ook iemand anders dan de CISO zijn. Alleen de CISO is echter bevoegd om te beoordelen of een melding anoniem kan worden verwerkt of niet. Een behandelaar dient dit dus altijd vooraf te overleggen alvorens een anonieme melding in behandeling te nemen.

informeren dat de status gaat worden gezien als afgehandeld. Dit geeft hen de gelegenheid nog in te grijpen. Indien zij nog wachten op verdere instructies informeert het de betrokkenen dat er geen verdere acties van hun kant worden verwacht.

10. **Behandelaar sluit het ticket en registreert het incident in het incidentenregister.**

Het incidentenregister maakt incidenten makkelijk doorzoekbaar op verschillende kenmerken. Tevens is het handig om te gebruiken voor rapportages en analyses. Deze kan meteen als het ticket aangemaakt wordt al worden geüpdate. Alleen het afhandelingsveld kan pas worden ingevuld als het incident is afgehandeld.

Algemene opmerkingen

- Wees positief tegen melders. Bedank hen voor de melding en laat blijken dat het melden belangrijk is en gewaardeerd wordt. Melden van incidenten willen we stimuleren, want het zorgt ervoor dat we passende actie kunnen ondernemen om schade te verkleinen of te voorkomen.
- Veroordeel melders niet. Incidenten veroorzaken is menselijk en kan iedereen overkomen. Toon daarom medeleven.
- In het verlengde van medeleven tonen; neem indien nodig de tijd om melders gerust te stellen of te troosten. Een incident kan een enorme mentale impact hebben op mensen. De behandelaar is veelal de eerste persoon die een melder spreekt en dient daarom daar rekening mee te houden en zich empathisch op te stellen.