Incidenten melden

Deze pagina bevat de volgende onderwerpen:

Terug naar homepagina Informatiebeveiliging

In geval van **aanwezigheid** CISO

Melden

Alle vragen en meldingen van (mogelijke) incidenten kun je doen via het mailadres 5.1.2.i @kiesraad.nl wanneer de CISO aan het werk is. Wacht hierna op instructies. Incidenten worden zo anoniem mogelijk geregistreerd en behandeld.

Dus wees een held; meldt!

Voor algemene vragen over de werkplek of ICT kan je de **SSC ICT servicedesk** bellen op: 070-4267447

In geval van **afwezigheid** CISO

Er is (mogelijk) sprake van een datalek/incident *binnen* de Kiesraad

Let op: betreft het een incident die een leverancier komt melden? Scroll dan verder naar beneden op deze pagina.

1. **Is de CISO (langer dan 24 uur) niet bereikbaar?**
   a. De CISO is langer dan 24 uur niet bereikbaar; *ga naar stap 2.*
   b. De CISO is korter dan 24 niet bereikbaar/is gewoon aan het werk; stuur een email naar 5.1.2.i @kiesraad.nl en wacht op verder contact.
2. **Wat is er aan de hand?**
   a. Er is sprake van een **storing/ICT probleem/ander soort beveiligingsprobleem** wat kan wachten tot de CISO terug is; stuur een email met uitleg over het incident naar 5.1.2.i 5.1.2.i @kiesraad.nl en bewaar alle relevante informatie en correspondentie (dus ook Signal/WhatsApp communicatie). Hou bij met wie, wanneer, waarover overleg is geweest en zet dat ook in de email. Als het inmiddels is opgelost, zet er dan ook bij wat de oplossing is geweest en wanneer het precies opgelost is.
   b. Er is sprake van een incident met een **fysieke component** (toegangspas verloren, toegangsdeur wil niet goed sluiten etc); meldt het incident bij de BVC 5.1.2.e 5.1.2.e en volg verder de instructies zoals bij 2a hierboven.
   c. Er is (mogelijk) sprake van een **datalek**; *ga naar stap 3.*
3. **Betreft het een datalek met persoonsgegevens?**
   a. **Persoonsgegevens** zijn alle gegevens die (in theorie) in de gelekte context door iemand (wie dan ook) te herleiden zijn naar de identiteit van een levend, natuurlijk persoon. Bijvoorbeeld: telefoonnummer, naam, adres, email adres, IP adres, ID nummer, schoenmaat, etc. Dat het voor een gemiddelde burger niet te herleiden is, is daarvoor niet relevant. Een IP adres kan een burger niet herleiden, maar een internetprovider bijvoorbeeld wel. Dat het IP adres gelekt is naar het internet, maakt daarvoor niet uit. Het is in theorie door iemand te herleiden en daarmee een persoonsgegeven. Neem maatregelen om het datalek te stoppen. Bij verkeerd verzonden emails; vraag de ontvanger de email te verwijderen en dit schriftelijk aan jou te bevestigen. Leg alle interne en externe communicatie vast als een soort logboek. Ook WhatsApp berichten.; *ga naar stap 4.*
   b. **Geen persoonsgegevens**; bepaal of er actie ondernomen moet worden om de impact te verkleinen/het lek te stoppen. Vraag bij verkeerd verzonden emails de ontvanger te bevestigen de mail te hebben verwijderd bijvoorbeeld. Bepaal of er impact te verwachten is voor de betrokkenen wiens informatie is gelekt (ook als het niet om persoonsgegevens, maar bijvoorbeeld zakelijke informatie gaat). Overleg in dat geval met het dienstdoende directielid wat je moet doen. Leg alles vast (communicatie intern, genomen stappen, mails etc) en stuur deze naar 5.1.2.i @kiesraad.nl. Zet erbij wanneer je met wie iets hebt besproken etc. Als een soort logboek.
4. **Maak een afweging omtrent de rechten en vrijheden van de betrokkene(n)**
   a. **Ik voorzie wel dat de betrokkene(n) in rechten en vrijheden beperkt kan worden**, dan wel last van ondervinden van dit datalek.; iemand kan bijvoorbeeld in de problemen komen omdat diens politieke voorkeur, BSN, mening, geloofsovertuiging, woonadres of andere informatie is gelekt. *ga naar stap 5.*
   b. **Ik voorzie dat de betrokkene(n) geen noemenswaardige inperking van rechten of vrijheden kan verwachten**, dan wel noemenswaardige hinder zal ondervinden van dit datalek. Overleg in dit geval met het dienstdoende directielid. Leg de afweging vast (waarom denk je dit?) en mail alles naar 5.1.2.i @kiesraad.nl.
5. **Indien de betrokkene(n) in rechten en vrijheden beperkt kan worden**:
   a. Overleg met het dienstdoende directielid en vertel dat mogelijk melden bij de Autoriteit Persoonsgegevens en/of betrokkenen zal moeten plaatsvinden.

    b. Neem contact op met de Functionaris Gegevensbescherming 5.1.2.e Vraag hem om advies.
    c. Leg alle overwegingen en besluiten vast. Bovenstaande moet binnen 72 uur na ontdekking van het datalek zijn voltooid ivm meldplicht.
    d. Indien wordt besloten melding te doen bij de AP; *ga naar stap 6.*
6. **Volg de instructies op de website van de AP en doe een voorinvulling.** Laat het betrokken directielid en de FG de voorinvulling goedkeuren voor verzending. Verzend de melding na goedkeuring. Stuur alle relevante informatie, communicatie (mail/weergave van telefonische of persoonlijke overleggen/WhatsApp gesprekken etc) naar 5.1.2.i @kiesraad.nl. Probeer hierbij een zo volledig mogelijke weergave te geven van het incident en hoe er is gehandeld in de tijd.
7. **Meld het datalek bij betrokkene(n)**
    a. **Er is 1 of meerdere bekende betrokkenen wiens contactgegevens bekend zijn bij ons**: informeer hen en geef aan welke activiteiten de betrokkene kan ondernemen om de impact te verkleinen.
    b. **Er zijn meerdere betrokkenen van wie wij geen contactgegevens hebben**; in dit geval dient er een bericht op een eenvoudig zichtbare plaats op onze website te worden geplaatst om eventuele betrokkenen te informeren.

Een leverancier wil een incident melden/ik kom er niet uit

Verwijs hen naar Office Management. Zij hebben mijn privé telefoonnummer en mogen deze met jou delen in dit geval.

Wees een Held; Meld!

In mei 2023 is de nieuwe procedure incidentmelden vastgesteld. Om deze bekend te maken is een kleine bewustwordingscampagne georganiseerd. Hieronder vind je daarvan de getoonde presentatie en het proces zelf.

Melden

Melden

Alle vragen en meldingen van (mogelijke) incidenten kun je doen via het mailadres 5.1.2.i @kiesraad .nl . Wacht hierna op instructies. Incidenten worden zo anoniem mogelijk geregistreerd en behandeld.

Dus wees een held; meldt!

Contact

Voor overige Informatiebeveiligingsvragen:

5.1.2.e

5.1.2.e @kiesraad.nl

Telefoon: 5.1.2.e

Functie: Chief Information Security Officer

Afdeling: Informatiebeveiliging

Tips

Op de hoogte blijven?

- Elke week op maandagochtend tussen 10:00 en 11:00 heeft de CISO, 5.1.2.e een spreekuur waarin ze vragen kan beantwoorden of jou meer vertellen over informatiebeveiliging. Vind haar in de bieb!
- Elke maand komt de Nieuwsbrief informatiebeveiliging uit op Confluence. Deze is binnen de Afdeling Informatiebeveiliging te vinden en voor iedereen te lezen: Nieuwsbrief - Kiesraad Wiki - SSC-ICT - Confluence (rijksweb.nl)
- Elke maand komt er een Rapportage informatiebeveiliging uit op Confluence. Deze zijn binnen de Afdeling Informatiebeveiliging te vinden en voor iedereen te lezen: Rapportages - Kiesraad Wiki - SSC-ICT - Confluence (rijksweb.nl)