

From: "5.1.2.e"
Sent: Wed, 26 Jan 2022 17:53:03 +0100
To: "5.1.2.e" <5.1.2.e@cbs.nl>; "Bruinsma, S.W.F.H. (Erik)" <5.1.2.e@cbs.nl>; "Kroese, A.H. (Bert)" <5.1.2.e@cbs.nl>
Subject: RE: Toelichting overleg datalekprocedure

Beste allen,

In aanvulling op 5.1.2.e's heldere overzicht: binnen de BIR heeft de functie van CISO betrekking op het zorgen voor een samenhangend systeem van maatregelen die dienen om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie binnen de organisatie te borgen. Daar valt niet alleen de IT-infra, maar de informatiehuishouding in brede zin onder. Niet alleen een verloren laptop, maar ook een vergeten dossier in de trein. Hoewel de component 'analoge' informatie-incidenten zal afnemen, blijven ze wel voorkomen, zo blijkt bijv. uit de constatering in de 27001-audit dat een kast met personeelsgegevens open was blijven staan.

De beoordeling of een informatie-incident een datalek (eigenlijk 'inbreuk') in de zin van de AVG is, hangt af of de rechten en vrijheden van betrokkenen in het geding zijn, en dat is alleen mogelijk als er persoonsgegevens in het spel zijn. Niet alle informatie-incidenten zijn datalekken in de zin van de AVG, maar alle datalekken in de zin van de AVG zijn wel informatie-incidenten. In navolging van het advies van 5.1.2.e ligt het dus in de rede alle informatie-incidenten in eerste instantie bij SSC te beleggen en op een subset daarvan een beoordeling door CPO (+evt. FG) te laten doen. In de drieliding die hieronder wordt gehanteerd: volgens mij zijn alle beveiligingsincidenten en facilitaire incidenten informatie-incidenten (en 'inbreuken' dus een subset daarvan).

Met vriendelijke groet,

5.1.2.e

5.1.2.e

CBS | Henri Faasdreef 312 | Postbus 24500 | 2490 HA Den Haag

M: 5.1.2.e | 5.1.2.e@cbs.nl

Volg [statistiekcb](#)s op twitter | facebook | instagram



Voor wat er **feitelijk** gebeurt

Van: 5.1.2.e <5.1.2.e@cbs.nl>

Verzonden: woensdag 26 januari 2022 14:42

Aan: Bruinsma, S.W.F.H. (Erik) <5.1.2.e@cbs.nl>; 5.1.2.e <5.1.2.e@cbs.nl>; 5.1.2.e <5.1.2.e@cbs.nl>

Onderwerp: Toelichting overleg datalekprocedure

Beste Erik en 5.1.2.e

Donderdag hebben we een overleg met elkaar omdat we willen afstemmen hoe en waar de verantwoordelijkheid van de datalekprocedure moet worden belegd.

Wat mij betreft wordt de vraag aan jullie: in welke hoofddirectie beleggen we de datalekprocedure?

Daar verschillen de meningen over. Ik heb heironder een hele uitgebreide toelichting, maar even heel in het kort:

- De CISO zou graag zien dat ik samen met de FG een functionele mailbox datalekken beheer, dat TOPdesk daarvoor een aparte button maakt en dat we meldingen over en weer via tickets doen (in plaats van mailverkeer). Dat laatste onderstreep ik, want dat is qua privacygevoeligheid ook beter.
- De FG 5.1.2.e geeft aan dat alle incidenten thuishoren bij SSC, dat zij verantwoordelijk zijn voor de rapportage over alle incidenten en dat incidenten over datalekken pas na afhandeling SSC naar ons toekomt. Hij geeft tevens aan dat daar een heel team zit terwijl ik in principe in mijn eentje ben, dus automatisch een risico.
- Ikzelf kijk vooral naar het praktische gedeelte. Ik wil graag de datalekprocedure verbeteren, ook de awareness hierover en ervoor zorgen dat medewerkers dit makkelijker gaan melden. Een stukje controle hierover en dus ook de verantwoordelijkheid hierover vind ik geen probleem mits we daar goede afspraken kunnen maken met het team van 5.1.2.e. Temeer omdat ik weet dat SSC geen actie onderneemt voor niet-IT gerelateerde incidenten.

Deze discussie afgelopen 2 maanden zorgde ervoor dat 5.1.2.e ik besloten hebben dit bij jullie neer te leggen.

5.1.2.e vul gerust aan!

Verdere toelichting.

Wat ik begreep is bij veel organisaties de verantwoordelijkheid van zowel informatiebeveiliging als privacy in de CIO office belegd (zowel de CISO als CPO zitten daar). Bij het CBS is dat gescheiden maar dat zorgt daardoor voor vragen rondom verantwoordelijkheid. De procedure en beschrijving is erg IT-gericht waardoor medewerkers binnen het CBS geen zicht hebben waar datalekken gemeld moeten worden.

Hieronder een situatieschets.

1. De huidige procedure is verouderd (2016) en moet geüpdatet worden.
2. Nu worden incidenten op verschillende plekken gemeld – we willen ernaartoe dat alles sowieso altijd gemeld wordt in Topdesk.
3. Na het melden in Topdesk bepaald SSC of een incident ook een datalek is en stuurt dat vervolgens door naar de FG.
4. Volgens SSC handelen ze geen incidenten af waar geen IT component aan zit.
5. De FG heeft afgelopen jaar een onderzoek gedaan naar het geringe aantal datalek meldingen en hiervoor aanbevelingen gedaan, komt erop neer dat niet alle datalekken gemeld of goed geregistreerd worden en de PDCA in Topdesk verbeterd moet worden;
6. In de privacy audit wordt geadviseerd dit advies op te volgen.

Ik heb de afgelopen maanden verschillende collega's gesproken w.o. 5.1.2.e en 5.1.2.e

Kort gezegd zijn er 3 soorten incidenten:

- Beveiligingsincidenten (al dan niet in relatie met andere 2).
- Facilitair (al dan niet met een relatie met andere 2).
- Datalekken (al dan niet in relatie met andere 2).

In de vernieuwde topdesk indeling zijn de eerste 2 categorieën wel als aparte button weergegeven, datalekken nog niet in afwachting van jullie beslissing.

5.1.2.e zou graag zien dat er voor datalekken een aparte button komt en dat de functionele mailbox door mij beheert wordt.

Volgens 5.1.2.e is dat zuiverder, worden incidenten transparanter afgehandeld omdat zichtbaar is waar het binnenkomt en welke route het aflegt.

Ik zou het zelf geen probleem 5.1.2.e omdat we vanuit privacy beter kunnen werken aan bewustwording en het melden van datalekken. Volgens de FG is de route echter altijd via SSC.

Poging tot phishing / melden van SPAM >

Virus melding >

Responsible disclosure (Melden kwetsbaarheid) >

Melden ander IT Beveiligingsissue >

Melden diefstal, vermissing en/of beschadiging >

Vriendelijke groet,

5.1.2.e

5.1.2.e

CBS | Henri Faasdreef 312 | Postbus 24500 | 2490 HA Den Haag

T 5.1.2.e / M 5.1.2.e | 5.1.2.e [@cbs.nl](mailto:5.1.2.e@cbs.nl)

Werkdagen ma t/m do

www.cbs.nl | twitter.com/statistiekcbs



Voor wat er **feitelijk** gebeurt