

Incident Response Plan (IRP)

Team P&S

28-3-2023 | Versienummer 1.1

Classificatie: Classificatiegroep 1 (Intern gebruik)

Versiebeheer

Versie	Datum	Wijziging	Auteur(s)
1.0	25-1-2022	Finalisering na akkoord directeur	M. Wieërs, privacy en security officer
Concept	8-3-2023	Afstemming met A. Baltus	M. Wieërs, privacy en security officer
1.1	28-3-2023	Finalisering na akkoord directeur	M. Wieërs, privacy en security officer

Goedkeuring/vaststelling

Gremium	Datum	Besluit
Directeur	28-3-2023	Akkoord

Rollen en verantwoordelijkheden

Aan het Incident response plan zijn een aantal rollen en verantwoordelijkheden verbonden. In de onderstaande tabel zijn de rollen en verantwoordelijkheden vertaald in een RASCI-tabel en zijn gekoppeld.

	Procesverantwoordelijke IT	Delivery Coördinator	Service management	Team P&S	Directie
Incident response plan	C	I	I	R	A

Inhoudsopgave

1. Relatie van dit plan met ISO27001	4
2. Inleidende opmerkingen	5
2.1 Doelstelling	5
2.2 Reikwijdte en beveiligingsprincipes	5
2.3 Algemene verantwoordelijkheid	6
3. Security gebeurtenissen en security incidenten	6
3.1 Wat is een security gebeurtenis?	6
3.2 Wat is een security incident?	6
3.3 Wat is een datalek?	7
4. Acties bij een security gebeurtenis en security incident	8
4.1 Actie Ontdekker: herkennen en melden	8
4.2 Meldingsproces	9
4.3 Wat te verzamelen?	9
5. Behandeling van de gebeurtenis	10
5.1 Verantwoordelijkheden ná melding	10
5.2 Incident response team (IRT)	10
5.3 Onderzoek	11
5.4 Verslaglegging en vastleggen bewijs	11
5.5 Communiceren en escaleren	11
5.6 Melding Autoriteit	11
5.7 Voorlopige Melding Autoriteit Persoonsgegevens	12
5.8 Melding bij betrokkenen	12
6. Rapportage	12
7. Monitoring	12
8. Evalueren en leren	13

1. Relatie van dit plan met ISO27001

Deze procedure is bedoeld als implementatie van de volgende ISO27001 beheersmaatregelen:

- **A.12.4.1 Gebeurtenissen registreren**
Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligings-gebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.
- **A.16.1.1 Verantwoordelijkheden en procedures**
Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatie-beveiligingsincidenten¹ te bewerkstelligen.
- **A.16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen**
Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.
- **16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging**
Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.
- **A.16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen**
Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.
- **A.16.1.5 Respons op informatiebeveiligingsincidenten**
Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.
- **A.16.1.6 Lering uit informatiebeveiligingsincidenten**
Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen, behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.
- **A.16.1.7 Verzamelen van bewijsmateriaal**
De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.
- **A.17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer**
Informatiebeveiligingscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.

¹ Binnen het VFPf wordt voor informatiebeveiligingsincidenten het woord 'Security incident' gehanteerd.

2. Inleidende opmerkingen

2.1 Doelstelling

De doelstelling van het VfPf bij dit plan is dat op alle bedreigende en versturende gebeurtenissen op systemen, de gegevens daarin en de daarvoor opgestelde processen zo snel mogelijk wordt geanticipeerd met de juiste maatregelen. Al deze gebeurtenissen worden altijd beoordeeld en geanalyseerd vanuit de standaard werkwijze in dit plan. Op deze manier is duidelijk waar en wanneer zich incidenten voordoen of voor hebben gedaan en of er sprake is van een datalek. Hoe helderder dit beeld, des te eerder en beter kunnen de juiste corrigerende of herstellende maatregelen worden getroffen en kan schade worden voorkomen.

In het kader van de plan-do-check-act-cyclus moet er ook lering worden getrokken uit alle gebeurtenissen om preventief betere maatregelen te implementeren om de frequentie, schade en kosten van toekomstige gebeurtenissen te voorkomen dan wel zoveel als mogelijk te beperken; dit leidt ook tot een verbetering van dit plan. Daarnaast draagt de cyclus bij aan borging van een zorgvuldige omgang met persoonsgegevens en wordt de verwijtbaarheid, aansprakelijkheid en gevolgschade voor betrokkenen voorkomen en/of geminimaliseerd.

2.2 Reikwijdte en beveiligingsprincipes

Dit document richt zich op het gehele proces van omgang met en beheersen van security gebeurtenissen en security incidenten (waaronder datalekken). In dit document leggen we het kader vast voor de melding, beoordeling en behandeling van security gebeurtenissen en security incidenten (waaronder datalekken) conform het beheer van informatiebeveiligingsincidenten uit de ISO27002.

Met dit plan wordt uitvoering gegeven aan het vastgestelde P&S-beleid en de hierin opgenomen fundamentele Beveiligingsprincipes om informatiebeveiliging effectief door te voeren binnen een organisatie, te weten:

- **Beschikbaarheid:** data/informatie en systemen/applicaties moeten op de juiste momenten Beschikbaar zijn: hebben gebruikers op de juiste momenten toegang tot de data/informatie en systemen/applicaties die ze voor hun werk nodig hebben?
- **Integriteit:** de data/informatie en systemen/applicaties moeten Integer zijn: is waar we mee werken en hoe we dat doen juist, is het volledig?
- **Vertrouwelijkheid:** de data/informatie en systemen/applicaties moeten Vertrouwelijk zijn en blijven waar dat nodig is: hebben alléén personen toegang tot data/informatie.

Er zijn situaties denkbaar waarbij de continuïteit van VfPf op het spel komt te staan omdat kritieke processen, diensten en/of producten niet meer beschikbaar zijn of bedreigd worden niet meer beschikbaar te zijn: dit noemen we een calamiteit. De gevolgen van calamiteiten voor de security maatregelen die VfPf heeft genomen heeft vallen buiten de scope van dit document en worden behandeld in het 'Bedrijfscontinuïteitsplan (BCP) VfPf V1.0'. Zodra tijdens de beoordeling in het kader van het Incident response plan blijkt van zo'n calamiteit, dan treden de acties van het BCP in werking; de acties uit het Incident response plan lopen waar nodig parallel hieraan.

Uit het Handboek P&S volgt dat security gebeurtenissen/incidenten niet als afwijkingen worden beschouwd. Afwijkingen komen voort uit interne audits, externe audits, document reviews en zijn afwijkingen die ontdekt worden door Team P&S, voordat een gebeurtenis zich voordoet. Incidenten kunnen wel het gevolg zijn van afwijkingen.

2.3 Algemene verantwoordelijkheid

Dit plan is gericht op iedereen die voor het VfPf werkt. In paragraaf 4 en 5 worden de verantwoordelijkheden verder uitgewerkt. Kortweg geldt dat het irrelevant is of een medewerker nu in vaste dienst is of op tijdelijke basis voor VfPf werkt dan wel voor een leverancier van VfPf werkt. Alle medewerkers en leveranciers zijn op de hoogte van deze werkwijze rondom security gebeurtenissen en security incidenten en melden deze gebeurtenissen.

3. Security gebeurtenissen en security incidenten

Er kan binnen dit plan op verschillende manieren sprake zijn van bedreigende en verstorende gebeurtenissen gericht op systemen, gegevens en processen van VfPf. In deze paragraaf wordt een onderverdeling aangebracht; al deze gebeurtenissen zijn in scope van dit plan en behoren te worden ontdekt, herkend, gemeld en behandeld.

3.1 Wat is een security gebeurtenis?

Het VfPf omschrijft een security gebeurtenis als een gebeurtenis die zich voordoet waarbij de Beschikbaarheid, Integriteit en/of Vertrouwelijkheid van systemen/applicaties en data/informatie van VfPf **mogelijk** in gevaar is of wordt gebracht. Het betreft de fase waarbij er twijfels zijn over een gebeurtenis en het nog niet duidelijk is of een dreiging zich daadwerkelijk heeft gerealiseerd of zal realiseren.

Bij een security gebeurtenis valt te denken aan de mogelijkheid van een zwakke plek/kwetsbaarheid in de informatiebeveiliging, een potentiële overtreding op het beleid voor informatiebeveiliging, een mogelijk falen van beveiligingsmaatregelen en/of een andere onbekende, onduidelijke of twijfelachtige situatie die relevant kan zijn voor de door VfPf getroffen Beveiligingsprincipes en beveiligingsmaatregelen.

Security gebeurtenissen kunnen zich ontwikkelen tot een security incident met als gevolg dat de belangen van VfPf in ernstige mate geraakt kunnen worden. Hierop moet tijdig en adequaat gereageerd worden. Alle gebeurtenissen worden daarom altijd beoordeeld en geanalyseerd. Dit onderzoek geeft uitsluitsel of de gebeurtenis effect heeft gehad op de genoemde Beschikbaarheid, Integriteit en/of Vertrouwelijkheid en of sprake is van een security incident.

3.2 Wat is een security incident?

Het VfPf omschrijft een security incident als een gebeurtenis die plaatsvindt door techniek of door (bewust of onbewust) menselijk handelen en die de Beveiligingsprincipes Beschikbaarheid, Integriteit en Vertrouwelijkheid van data/informatie² en/of de systemen/applicaties dan wel de processen van VfPf **daadwerkelijk** in gevaar brengt (poging), heeft gebracht, heeft misbruikt of heeft verstoord.

Het gaat hierbij om fysieke en digitale inbrekers, kwetsbaarheden/zwakke plekken in systemen/applicaties van VfPf of virussen op het netwerk, maar ook om langdurige (stroom-)storingen, het verlies van documenten, het achterlaten van een vertrouwelijk document bij een printer of het ontbreken (of fout lopen) van een back-up met als gevolg het niet beschikbaar zijn van gegevens.

² Met data/informatie worden de categorieën bedoeld zoals omschreven in het Classificatiebeleid, te weten de Informatiegroepen: openbaar, intern gebruik, bedrijfsvertrouwelijk en vertrouwelijk.

Ook de volgende situaties zijn security incidenten:

- *Alle hackpogingen (gelukt of mislukt) en DDoS aanvallen, of autorisaties die ten onrechte verleend maar niet gebruikt zijn*
- *Een phishing mail die is ontvangen;*
- *Een phishing mail waarbij op de bijlage is gedrukt of de link is geopend;*
- *Het langdurig (ongeaccepteerde overschrijding van in afspraken vastgelegde downtime) niet beschikbaar en/of toegankelijk zijn van gegevens en systemen/applicaties voor VfPf en voor schoolbesturen;*
- *Een malware-besmetting;*
- *Een handeling wordt verricht in strijd met richtlijnen en/of beleid zoals de Gedragscode uit het Personeelshandboek;*
- *Inbreuk op fysieke beveiligingsvoorzieningen;*
- *Toegangsovertredingen;*
- *Beschadigen of vernielen van (kritische) apparatuur;*
- *Onbevoegd inzien van vertrouwelijke informatie;*
- *Onbedoelde openbaarmaking van bedrijfsvertrouwelijke vertrouwelijke informatie;*
- *E-mail met onversleutelde bedrijfsvertrouwelijke informatie;*
- *Kenbaar maken (waaronder uitwisselen) van of onzorgvuldig omgaan met wachtwoorden;*
- *Etc.*

3.3 Wat is een datalek?

Van een datalek (in de zin van artikel 4 sub 12 van de Algemene verordening gegevensbescherming) is sprake als er bij een security incident ook persoonsgegevens³ zijn betrokken. Een datalek is dus een speciale vorm van een security incident.

Bij een datalek speelt de situatie dat een inbreuk op de persoonsgegevens per ongeluk of bewust op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van die persoonsgegevens. Een datalek is dus ook altijd een security incident. In sommige gevallen moet zo'n datalek worden gemeld bij de Autoriteit Persoonsgegevens (AP) en soms óók bij de betrokkenen om wiens gegevens het gaat.

Voorbeelden van datalekken zijn:

- *het verlies van niet-versleutelde persoonsgegevens;*
- *een cyberaanval waarbij persoonsgegevens zijn buitgemaakt, of zijn benaderd;*
- *een besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn gemaakt;*
- *een e-mail met persoonsgegevens is (onbeveiligd) verzonden naar een verkeerd mailadres;*
- *verzending van bulk e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden;*
- *een account wordt aangemaakt voor een verkeerde gebruiker waardoor onbevoegde inzage plaatsvindt van persoonsgegevens;*
- *Achtergelaten kopie met persoonsgegevens in de printer;*
- *Onbedoelde doorgifte van gegevens aan een betrouwbare derde;*
- *Fout bij bezorging per post;*
- *Een door VfPf gecontracteerde dienstverlener deelt informatie met persoonsgegevens met de verkeerde persoon;*
- *Etc.*

³ Volgens artikel 4, sub 1, AVG wordt onder een persoonsgegeven verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Een datalek kent drie varianten⁴:

- er is sprake van een datalek, maar hoeft **niet** te worden gemeld bij de Autoriteit Persoonsgegevens (de AP) omdat het onwaarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van betrokkenen inhoudt;
- er is sprake van een datalek, dat **wél** gemeld moet worden bij de AP omdat het waarschijnlijk is dat de inbreuk **een risico** voor de rechten en vrijheden van betrokkenen inhoudt;
- er is sprake van een datalek, dat **wél** gemeld moet worden bij de AP **én** bij betrokkene(n) omdat het waarschijnlijk is dat de inbreuk **een hoog risico** voor de rechten en vrijheden van betrokkenen inhoudt.

4. Acties bij een security gebeurtenis en security incident

4.1 Actie Ontdekker: herkennen en melden

In de keten van VfPf hebben in ieder geval de volgende afdelingen en personen de verantwoordelijkheid security gebeurtenissen en security incidenten te herkennen, ontdekken en te melden bij Team P&S:

- **Alle interne en externe medewerkers VfPf:** dit zijn alle medewerkers binnen alle gelederen en afdelingen van VfPf die zich met de dagdagelijkse werkzaamheden en dienstverlening bezig houden.
- **Medewerkers van de helpdesk (WWplus):** schoolbesturen nemen om verschillende redenen contact op met de helpdesk en de helpdeskmedewerker legt elke melding vast in het Klantregistratiesysteem; voor elke melding die technisch van aard is wordt een Topdesk-melding aangemaakt.
- **Leden van Team P&S:** eigen waarneming dan wel het contactpunt binnen kantooruren per e-mail en 24/7 beschikbaar via in ieder geval telefoon.
- **Medewerkers bij leveranciers:** dit zijn medewerkers bij opdrachtnemers en/of Verwerkers die de systemen/applicaties voor VfPf hosten en beheren. Met deze partijen zijn afspraken gemaakt over de melding van security gebeurtenissen en datalekken en vastgelegd in Verwerkersovereenkomsten. Leveranciers melden alle gebeurtenissen en zwakke plekken binnen 24 uur nadat de gebeurtenis of zwakke plek is ontdekt in ieder geval telefonisch bij Team P&S.
- **automatische response vanuit systemen/applicaties:** beheerders van systemen/applicaties die van een automatisch alarmsysteem zijn voorzien en die bij specifieke events berichten stuurt naar medewerkers van het IV Regieteam, servicemanagers en/of naar leveranciers.

Buiten de hierboven genoemde categorieën bestaat ook de mogelijkheid dat kwetsbaarheden en dreigingen door **NCSC** en **OCW** gemeld kunnen worden. Daarnaast kunnen meldingen binnenkomen via het door VfPf ingeschakelde '**Security.txt**'.

⁴ Bij het bepalen of sprake is van een datalek en de inhoudelijke beoordeling daarvan, hanteert Team P&S de van toepassing zijnde richtsnoeren voor het melden van inbreuken (waaronder in ieder geval: 'Guidelines on Personal data breach notification under Regulation 2016/679' én 'Guidelines 01/2021 on Examples regarding Data Breach Notification').

4.2 Meldingsproces

Het meldingsproces is een gezamenlijke verantwoordelijkheid waarbij de eerste lijn en de tweede lijn samen het proces rondom ontdekken, melden en afhandelen oppakken.

Team P&S is het vaste contactpunt om security gebeurtenissen en security incidenten bij te melden, heeft de lead in het (beoordelings)proces- en onderzoek en is 24/7 beschikbaar om deze gebeurtenissen in behandeling te nemen.

Medewerkers melden alle security gebeurtenissen en security incidenten meteen, maar niet later dan een uur nadat de gebeurtenis is ontdekt, telefonisch bij Team P&S. Deze medewerker brengt ook de ketenverantwoordelijke - en indien sprake is van systemen/applicaties van VfPf - de Procesverantwoordelijke IT van IV-Regieteam op de hoogte van de gebeurtenis.

Leveranciers melden alle security gebeurtenissen en security incidenten binnen 24 uur nadat de gebeurtenis is ontdekt aan de ketenverantwoordelijke van de van toepassing zijnde afdeling waarbinnen de situatie zich voordoet, de verantwoordelijke medewerker binnen het IV-Regieteam én bij Team P&S.

4.3 Wat te verzamelen?

De ontdekker van een security gebeurtenis of security incident verzamelt zoveel mogelijk informatie. Als Team P&S vaststelt dat onvoldoende bewijsmateriaal voorhanden is, dan worden aanvullende vragen uitgezet bij de ontdekker of andere personen om ontbrekend bewijs zo snel mogelijk te verzamelen. De volgende informatie wordt – voor zover mogelijk - direct verzameld:

- *de naam van de persoon en contactgegevens van de persoon die de melding doet;*
- *de datum en tijd waarop de melder de gebeurtenis heeft ontdekt en gemeld heeft aan Team P&S;*
- *korte beschrijving hoe de gebeurtenis ontdekt is;*
- *wat is de oorzaak van de gebeurtenis?*
- *wat is de aard van de inbreuk? (inbreuk op toegang tot, juistheid van en/of beschikbaarheid van data/informatie)*
- *wat voor soort data/informatie is betrokken bij de gebeurtenis? Interne, bedrijfsvertrouwelijke of vertrouwelijke informatie? En wat voort soort informatie daarbinnen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens et cetera);*
- *wie zijn de betrokkenen?*
- *de datum en tijdstip (volledige duur van begin tot eind) van de gebeurtenis;*
- *welke systemen/applicaties zijn bij de gebeurtenis betrokken en in welke vorm zijn data/informatie opgeslagen (op papier, digitaal, op een verwijderbare gegevensdrager?*
- *welke leverancier(s) en andere ketenpartner(s) is/zijn bij de gebeurtenis betrokken?*
- *duurt de gebeurtenis nog voort of is deze gestopt en zo ja, hoe?*
- *om hoeveel records van data/informatie en om hoeveel betrokkenen ?*
- *indien mogelijk, een beschrijving welke technische beveiligingsmaatregelen aanwezig zijn (zoals versleuteling, afgeschermd omgevingen etc.);*
- *wat is naar de opvatting van de melder de ernst van de gevolgen voor betrokkenen?*

5. Behandeling van de gebeurtenis

5.1 Verantwoordelijkheden ná melding

De bij de security gebeurtenis of het security incident betrokken functionarissen behandelen in teamverband de melding en zoeken gezamenlijk naar de juiste oplossing om de inbreuk te stoppen, te beperken, de schade in te dammen en deze (zoveel als mogelijk) te herstellen. Het betreft hier de behandeling van gebeurtenissen waarvoor een Incident response team niet opgericht hoeft te worden.

In samenspraak met de Procesverantwoordelijke IT (als de gebeurtenis ziet op systemen/applicaties) en/of met de betrokken verantwoordelijke personen uit de van toepassing zijnde afdeling, bepaalt Team P&S zo snel als mogelijk of de gebeurtenis als een security gebeurtenis of als security incident conform paragraaf 3.1 gekwalificeerd moet worden. Team P&S heeft daarnaast een adviserende rol.

Het IV-Regieteam biedt ondersteuning bij het onderzoeken van security gebeurtenissen en security incidenten en waar nodig het implementeren van verbetermaatregelen. Indien nodig bepaalt de Procesverantwoordelijke IT of andere leden uit het IV-Regieteam moeten worden aangehaakt.

De ketenverantwoordelijke is eindverantwoordelijk voor het oplossen van een security gebeurtenis of een security incident. De ketenverantwoordelijke is verantwoordelijk voor een gepaste beveiliging van de onder zijn/haar verantwoordelijkheid uitgevoerde processen en de daarbij gebruikte processen, systemen/applicaties en data/informatie en verleent alle medewerking bij de analyse van het incident en de implementatie van de verbetermaatregelen.

5.2 Incident response team (IRT)

Het oprichten van een IRT is afhankelijk van de aard, omvang, ernst en impact van de gebeurtenis op de inbreuk op de Beschikbaarheid, Integriteit en Vertrouwelijkheid. De samenstelling van het IRT kan daarom wisselen. Het gaat dan om een security gebeurtenis of security incident met een hoge impact op de bedrijfsvoering van VfPf of het dagelijks leven van betrokkenen, waarbij directe mobilisering van het IRT vereist is.

Team P&S besluit, in samenspraak met de betrokken personen uit de van toepassing zijnde in- en externe afdelingen (zie paragraaf 5.1), of een IRT moet worden opgericht. Team P&S coördineert en faciliteert de samenwerking van het IRT. Team P&S heeft daarnaast ook hier een adviserende rol.

In het IRT neemt altijd de ketenverantwoordelijke zitting; wanneer de gebeurtenis ziet op systemen/applicaties dan is altijd een lid van het IV-Regieteam aanwezig en deze wordt door de Procesverantwoordelijke IT beschikbaar gesteld.

Het IRT onderzoekt altijd de oorzaak van de gebeurtenis. Team P&S beoordeelt, in samenspraak met de leden van het IRT, van welke gradatie als bedoeld in paragraaf 3 sprake is. Indien nodig, bepaalt het IRT welke technische en organisatorische maatregelen nodig zijn om de inbreuk en de daaraan ten grondslag liggende kwetsbaarheid en zwakke plek te verhelpen, de inbreuk te stoppen en eventuele verdere inbreuk en schade te voorkomen. Binnen het IRT neemt de ketenverantwoordelijke een besluit over de te nemen beheersmaatregelen.

Als uit het security incident direct schade voortvloeit voor betrokkene(n) en/of VvPf dan worden door het IRT onmiddellijk passende maatregelen getroffen om de schade te beperken, te beëindigen en te herstellen. De directeur (en het MT) wordt op de hoogte gesteld van de maatregelen.

5.3 Onderzoek

Er wordt een (forensische) oorzaak- en omvanganalyse uitgevoerd om de bron en oorzaak van de security gebeurtenis of het security incident te achterhalen en te (laten) verhelpen. In de regel wordt de oorzaakanalyse uitgevoerd door de ketenverantwoordelijke, tenzij de ketenverantwoordelijke een andere persoon daartoe aanwijst.

5.4 Verslaglegging en vastleggen bewijs

Bij de vastlegging van gebeurtenissen wordt altijd het template 'Logboek security gebeurtenissen' (logboek) gehanteerd.⁵ Team P&S documenteert tijdens het beoordelingsproces alle relevante feiten, activiteiten en bewijsstukken, waaronder in ieder geval de toedracht, de beoordeling, besluit(en) en getroffen maatregelen inclusief de relevante e-mails.

Team P&S maakt hiervoor een opslaglocatie aan op de "Werkmap Privacy en Security - Documenten\17. Datalekken en incidenten". Dit document wordt gedeeld met de bij de security gebeurtenis/incident betrokken personen.

5.5 Communiceren en escaleren

De directeur (en het MT) wordt van de oprichting van een IRT zo snel mogelijk, maar in ieder geval op de dag van oprichting, op de hoogte gesteld. Ook de Functionaris voor gegevensbescherming (FG) wordt geïnformeerd. De directeur wordt vervolgens tussentijds geïnformeerd over de ontwikkeling van de security gebeurtenis of het security incident. Indien nodig, wordt afdeling Communicatie ook van de oprichting van het IRT op de hoogte gesteld; overige betrokkenen worden op basis van 'need-to-know' geïnformeerd.

Van security gebeurtenissen waarvan op voorhand niet duidelijk is of de gebeurtenis organisatiebreed impact heeft en uitgesloten moet worden dat sprake is van een security incident, wordt de directeur (en het MT) geïnformeerd.

Als Team P&S dan wel het IRT concludeert dat andere in- en externe personen of organisaties op de hoogte gesteld moeten worden van het bestaan van het security incident (of relevante details daarvan) dan communiceert Team P&S dat richting die personen en/of organisaties.

Als Team P&S dan wel het IRT constateert dat bepaalde activiteiten en/of handelingen van Team P&S of het IRT op enigerlei wijze belemmerd of verstoord worden, dan escaleert Team P&S naar de directeur.

5.6 Melding Autoriteit Persoonsgegevens

Als Team P&S vaststelt, in samenspraak met de IRT-leden, dat sprake is van een meldingsplichtig datalek, dan informeert Team P&S de Autoriteit Persoonsgegevens binnen 72 uur (kalenderuren).

⁵ Uitzondering hierop zijn phishingberichten als deze slechts gemeld worden; als op de phishing is geantwoord (door het drukken op een verdachte link, het openen van een onbetrouwbare bijlage etc.) dan wordt dit incident verder uitgewerkt in het logboek.

Met de directeur volgt eerst afstemming en met de FG volgt consultatie. Na akkoord van de directeur wordt door Team P&S een melding gedaan bij de Autoriteit Persoonsgegevens via het daarvoor bestemde loket.

5.7 Voorlopige Melding Autoriteit Persoonsgegevens

De mogelijkheid kan zich voordoen dat Team P&S dan wel het IRT niet binnen 72 uur kan vaststellen dat sprake is van een meldingsplichtig datalek als bedoeld in paragraaf 3.3. Om de termijn te bewaken wordt het security incident in dat geval voorlopig aangemerkt als een meldingsplichtig datalek. Met de directeur volgt eerst afstemming en met de FG volgt consultatie. Na akkoord van de directeur wordt door Team P&S een voorlopige melding gedaan bij de Autoriteit Persoonsgegevens via het daarvoor bestemde digitale loket.

5.8 Melding bij betrokkenen

Als Team P&S vaststelt, in samenspraak met de IRT-kleden, dat sprake is van een meldingsplichtig datalek dat óók bij betrokkenen moet worden gemeld, dan wordt in samenspraak met de afdeling Communicatie de wijze bepaald waarop de betrokkenen geïnformeerd worden. Met de directeur volgt afstemming en met de FG volgt consultatie.

Betrokkene wordt altijd zo snel mogelijk geïnformeerd over wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn. Ook wordt betrokkene geïnformeerd over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen. Onder bepaalde voorwaarden hoeft een melding aan betrokkene(n) niet plaats te vinden.⁶

6. Rapportage

Periodiek wordt de directeur middels de kwartaalrapportage geïnformeerd over security gebeurtenissen en security incidenten in de achterliggende periode. De rapportage wordt vervolgens in de eerstvolgende MT-vergadering ter kennisgeving aan het MT aangeboden.

7. Monitoring

In het logboek wordt vastgelegd welke actiehouders verantwoordelijk is voor het realiseren van acties en maatregelen en binnen welke tijdsbestek de maatregel geïmplementeerd wordt.

Team P&S registreert de beheersmaatregelen in het Incidentenregister en monitort de voortgang vanuit de Operationele Planning in de Jaarkalender en volgt de voortgang. Indien nodig en afhankelijk van die voortgang stelt Team P&S interventies voor dan wel adviseert bijsturende acties om de doelstelling te bereiken van het implementeren van de beheersmaatregelen.

Een security gebeurtenis en een security incident wordt formeel afgesloten nadat de gebeurtenis of het incident is behandeld.

⁶ In artikel 34, lid 3 van de AVG zijn drie voorwaarden opgenomen waaronder geen mededeling vereist is.

8. Evalueren en leren

De organisatie wil leren van incidenten, en daarom moeten incidenten geëvalueerd worden.

Periodiek vindt een evaluatie van elk security incident plaats, conform de planning in de Operationele Planning van de Jaarkalender. Van de kennis die is verkregen door de security gebeurtenis of het security incident te analyseren en op te lossen wordt lering getrokken (worden trends ontdekt) door deze te gebruiken om de waarschijnlijkheid of impact van toekomstige incidenten te identificeren, te verkleinen en om zwakke plekken en kwetsbaarheden in bestaande (primaire) processen en architectuur te voorkomen, op te lossen en te verbeteren.

Als uit de evaluatie blijkt dat uitgebreidere of aanvullende beheersmaatregelen nodig zijn om de frequentie, schade en kosten van toekomstige gebeurtenissen te beperken, dan worden deze ingezet na goedkeuring van de ketenverantwoordelijke.

De praktijksituaties van security gebeurtenissen en security incidenten worden gebruikt in een gebruikersbewustzijnstraining als voorbeelden van wat kan gebeuren, hoe te reageren op dergelijke incidenten en hoe deze in de toekomst voorkomen kunnen worden.

Als uit de evaluatie blijkt dat dit Incident respons plan direct gewijzigd moet worden, dan wordt dit direct meegenomen en wordt dit document herijkt.

Tot slot is het belangrijk om de melder een terugkoppeling te geven over de uitkomsten van de gebeurtenis of het incident. Zo wordt het signaal afgegeven dat melden loont.
