Beveiligingsincidenten

Procedure beveiligingsincidenten MeanderGroep

Inleiding

Binnen Meander worden veel vertrouwelijke gegevens verwerkt, zoals klantgegevens, gegevens over de omgeving van de cliënt en medewerkergegevens. Er worden veel maatregelen genomen om deze gegevens te beschermen, maar desondanks kan het voorkomen dat de gegevens in verkeerde handen terecht komen. In dit protocol wordt beschreven hoe gehandeld moet worden als dit zich voordoet.

1. Wat is een beveiligingsincident

Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen. Enkele voorbeelden van beveiligingsincidenten zijn:

- ✓ besmettingen met virussen en/of malware,
- ✓ diefstal / verlies van laptop, IPAD, USB stick, mobiele telefoon,
- ✓ onjuiste adressering van e-mail of post,
- ✓ een open papiercontainer met vertrouwelijke gegevens,
- ✓ ongeautoriseerde toegang tot vertrouwelijke gegevens,
- ✓ te veel rechten,
- ✓ phishing emails of telefoontjes,
- ✓ het delen van wachtwoorden,
- ✓ diefstal / verlies van cliëntendossiers.

2. Melding van een beveiligingsincident

Beveiligingsincidenten dienen zo snel mogelijk te worden gemeld bij de ICT Servicedesk. Deze is bereikbaar via ServicedeskI&A@mgzl.nl, of via telefoonnummer 045 5616115.

3. Procedure

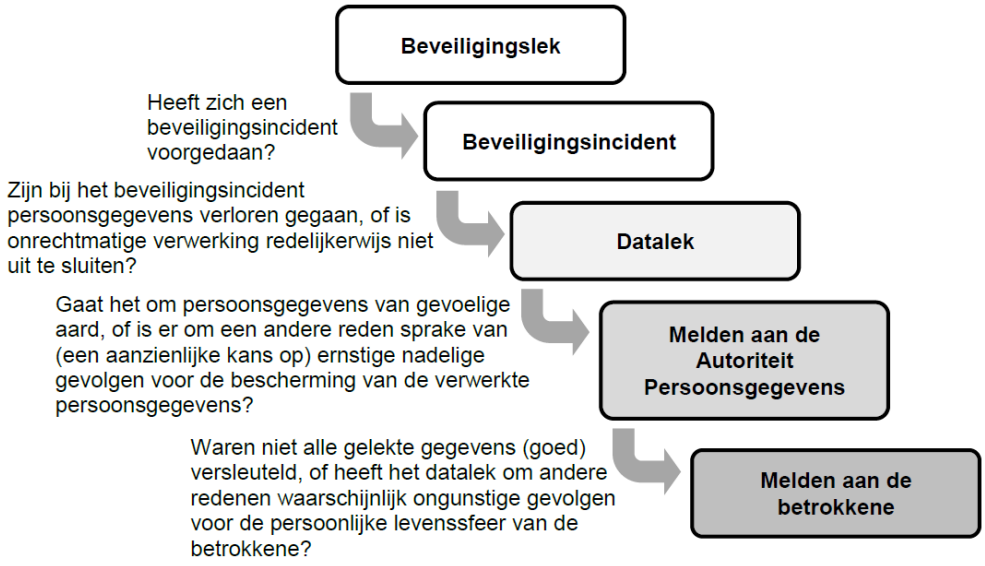
De procedure na de melding van een beveiligingsincident bij Meander, is weergegeven in een beslismodel (zie figuur 1).

Degene die het incident registreert neemt eerst alle maatregelen die binnen zijn eigen invloedssfeer liggen. De ict-servicedesk zorgt ervoor dat eerst beoordeeld wordt of er nog technische maatregelen genomen dienen te worden om het incident te stoppen en/of de schade kunnen beperken. Indien verder onderzoek nodig is wordt het incident doorgegeven aan de Information Security Officer. Deze verzamelt alle noodzakelijke gegevens voor een impactbepaling voor zover deze nog niet beschikbaar zijn. Op basis hiervan maakt hij een inschatting of het een datalek betreft en of gevoelige persoonsgegevens (afhankelijk van aard en context) zijn gelekt. Is dit het geval, dan wordt het incident geëscaleerd naar Functionaris Gegevensbescherming.

melding AP:
Als blijkt dat er een meldplicht is dan informeert de functionaris gegevensbescherming de AP over het datalek.

informatieplicht aan betrokkene
Is er een informatieplicht aan de betrokkene, dan moet dit onverwijld gemeld worden. Na het ontdekken van het datalek mag nog enige tijd genomen worden voor nader onderzoek zodat betrokkene op een behoorlijke en zorgvuldige manier geïnformeerd wordt. De functionaris gegevensbescherming bepaalt in overleg met de afdeling Communicatie hoe hier het beste invulling aan kan worden gegeven. In de kennisgeving dient in elk geval te worden vermeld: de aard van de inbreuk, de instanties waar betrokkene meer informatie kan krijgen, de contactgegevens van Meander en maatregelen die worden aanbevolen aan betrokkene om de negatieve gevolgen van het lek te beperken, bijvoorbeeld het veranderen van gebruikersnamen en wachtwoorden.

Figuur 1: Beslismodel Beveiligingsincidenten



4. Registratie beveiligingsincidenten

De security officer houdt een overzicht bij van alle beveiligingsincidenten en datalekken. Elk incident bevat het overzicht van de feiten en gegevens over de aard van de inbreuk en de genomen maatregelen. Als het datalek is gemeld aan de betrokkene, dan wordt ook de tekst van de kennisgeving aan de betrokkene in het overzicht opgenomen. Van elk incident wordt een incidentrapportage gemaakt die door de raad van bestuur wordt vastgesteld.
De bewaartermijn van het overzicht incidenten is minimaal een jaar. In bepaalde gevallen kan het nodig zijn om een langere bewaartermijn te hanteren.
Het overzicht is voor intern gebruik binnen Meander en wordt niet openbaar gemaakt.

5. Contactgegevens

De raad van bestuur van Meander is verantwoordelijke in de zin van de Wet bescherming persoonsgegevens en eindverantwoordelijk voor de juiste afhandeling van een vermoedelijk datalek. De raad van bestuur mandateert de volgende functionarissen om namens Meander alle handelingen te verrichten die noodzakelijk zijn in het kader van de meldprocedure voor een vermoedelijk datalek: functionaris gegevensbescherming.