Lering trekken uit eerdere datalekken

Het is belangrijk dat organisaties het bijhouden van het datalekregister niet uitsluitend als een administratieve verplichting zien, maar ook als middel om te leren van eerdere incidenten. De AP geeft hierbij een voorbeeld van een stappenplan dat organisaties periodiek kunnen uitvoeren als onderdeel van de plan-do-check-act (PDCA-)cyclus. Dit stappenplan kunnen zij gebruiken om bij te houden of (bepaalde typen) datalekken toenemen, wat daar de mogelijke oorzaak van is, of eerder genomen maatregelen hebben gewerkt om het aantal datalekken te verminderen en of er aanvullende maatregelen nodig zijn. Zo kunnen organisaties de beveiliging van persoonsgegevens voortdurend evalueren en verbeteren.

STAP 1: Maak een analyse op basis van het datalekregister

- Hoeveel datalekken hebben de afgelopen periode plaatsgevonden?
- Om wat voor type datalekken ging het? Welke type datalekken komt het meest voor?
- Welke type datalekken levert het hoogste risico op voor slachtoffers?

Vergelijk met voorgaande perioden: zijn er opvallende trends zichtbaar?

- Is het aantal (ernstige) datalekken toegenomen of afgenomen?
- Zijn er de afgelopen periode meer datalekken gemeld aan de AP en aan de slachtoffers?
- Is er een toename of afname zichtbaar in bepaalde type datalekken?
- Wat is de mogelijke oorzaak van de toename of afname?

Let op: toename of afname in het aantal (gemelde) datalekken kan ook zijn veroorzaakt doordat in de afgelopen periode intern meer of minder datalekken zijn gemeld/geregistreerd dan daarvoor.

STAP 2: Bekijk welke maatregelen u kunt nemen om het risico op de ernstigste en/of veelvoorkomende datalekken te beperken

Geef prioriteit aan maatregelen gericht tegen datalekken die het hoogste risico opleveren, en aan relatief eenvoudig te nemen maatregelen die waarschijnlijk direct effect zullen hebben ('laaghangend fruit').

STAP 3: Monitor de implementatie van de voorgenomen (aanvullende) beveiligingsmaatregelen

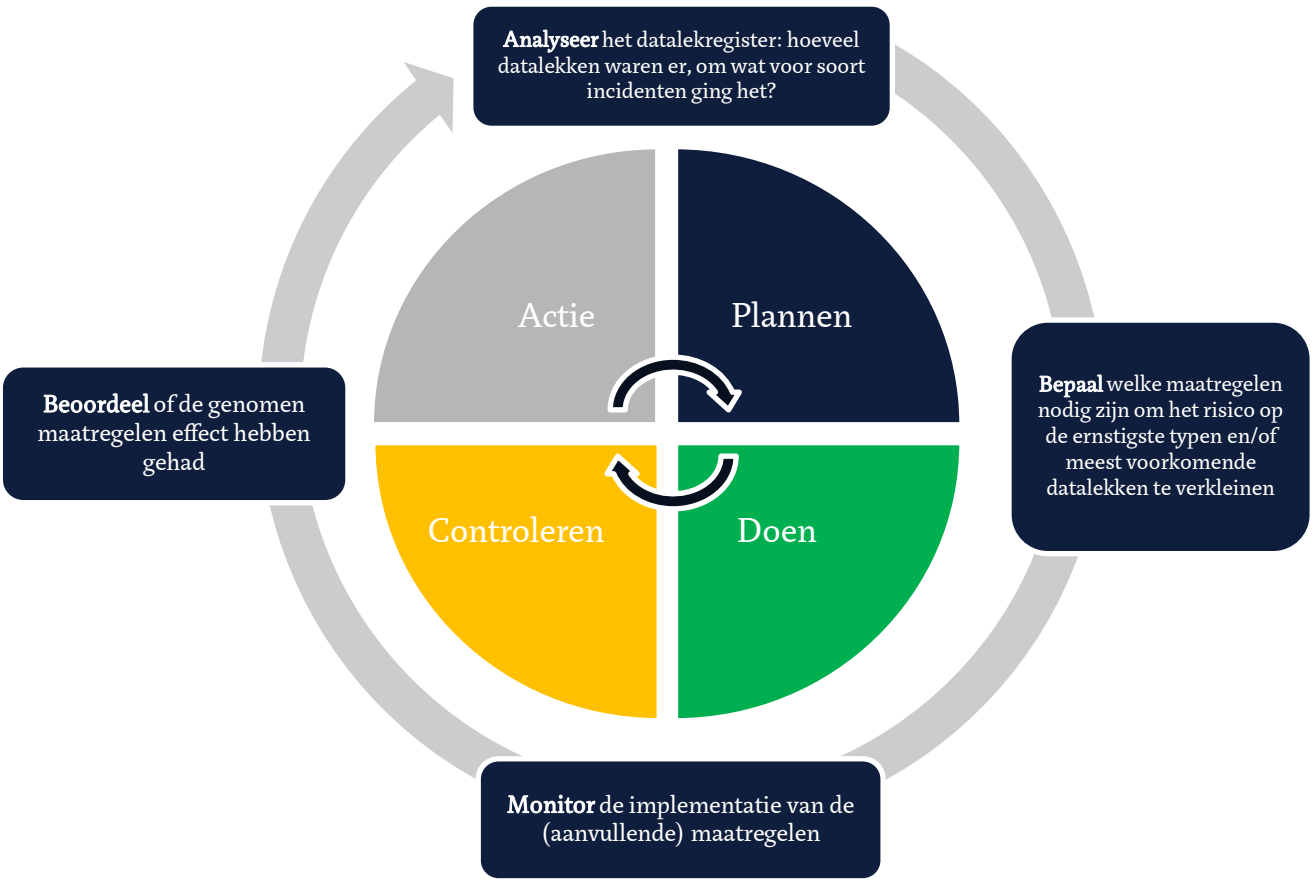
- Zijn de aangekondigde maatregelen uit de vorige cyclus inmiddels ingevoerd?
- Zo niet, hoe komt dat? Wanneer worden deze maatregelen alsnog uitgevoerd?

Zijn voorgenomen beveiligingsmaatregelen niet binnen de afgesproken periode geïmplementeerd? Spreek het verantwoordelijke management hierop aan en maak hierover afspraken.

STAP 4: Beoordeel (bijvoorbeeld: na een half jaar) of de genomen aanvullende maatregelen effect hebben gehad

- Hebben de maatregelen die tijdens de vorige cyclus zijn ingevoerd geleid tot een afname van het aantal datalekken (van een bepaald type)?
- Als de maatregelen niet effectief zijn gebleken, waar lag dat aan? Zijn er aanvullende maatregelen nodig?

Herhaal de stappen 1 t/m 4 elk jaar of elk half jaar en rapporteer hierover aan het hoogste management. De AP raadt aan om de FG en de CISO te betrekken bij de uitvoering van deze stappen.


Analyseer het datalekregister: hoeveel datalekken waren er, om wat voor soort incidenten ging het?
Actie
Plannen
Controleren
Doen
Bepaal welke maatregelen nodig zijn om het risico op de ernstigste typen en/of meest voorkomende datalekken te verkleinen
Monitor de implementatie van de (aanvullende) maatregelen
Beoordeel of de genomen maatregelen effect hebben gehad