Een datalek/incident dat zich heeft voorgedaan bij de klant zelf

Voorbeelden voor 'externe' datalekken: een gestolen/verloren zakelijke laptop, telefoon, USB-stick of andere opslag devices, per ongeluk delen van (persoons)gegevens van derden, phishing en ransomware, papieren met gegevens niet vernietigd (denk aan papierbak, postvakjes zonder beveiliging).
Ook al zijn wij niet verantwoordelijk voor het lek, als automatiseerder willen wij een adviserende rol aannemen en reageren door direct actie te ondernemen op de technische kant ter voorkoming van meer schade of het herstel (van diensten/producten die wij zelf hebben geleverd).

Klant geeft aan dat er een incident heeft voorgedaan. Je reageert direct door vragen te stellen:

1. **Wat houdt het lek in?:**
   Wat is er exact gebeurd, bij wie of wat heeft het incident zich voorgedaan? In hoeverre zijn wij betrokken bij het lek òf het oplossen hiervan?

2. **Wie is de contactpersoon bij de klant en bij ons intern om zaken omtrent het datalek te bespreken?**
   Zorg dat er bij beiden één hoofdcontactpersoon is, wie dat zijn en dat intern iedereen op de helpdesk op de hoogte is.

3. **Geef aan de klant aan dat zij melding van datalekken moeten doen bij Autoriteit Persoonsgegevens**
   Let op: Verplicht is het documenteren van datalekken!

4. **Wie zijn de betrokkenen?:**
   Hebben hun klanten hinder hiervan? Adviseer dan dat jouw klant een datalek of incident zo snel mogelijk aan de betrokkenen meldt!

5. **Zijn er accounts, mailboxen of systemen aangetast?:**
   Bekijk welke accounts eventueel geblokkeerd kunnen worden, bespreek dit met de contactpersoon. Geef het duidelijk aan als er tijdelijk geen werkzaamheden gedaan kunnen worden rondom deze accounts/systemen.

6. **Indien back-up:** Geef aan dat je de back-up shadowcopy terugzet indien dit mogelijk is (bij phishing mail ransomware eerst bekijken en overleggen wat de gevolgen zijn)

7. **Geef een tijdsindicatie betreft het zo snel mogelijk weer werkende maken van betrokken accounts/systemen:** Indien niet alle details bekend zijn, vertel dan de details die wel bekend of waarschijnlijk zijn, wat de organisatie doet om de ontbrekende informatie te achterhalen en wanneer we met een update komen.

8. **Benadruk dat de situatie kan veranderen:** Omdat datalekken complex van aard zijn, is het van belang aan te geven dat de situatie kan veranderen met kwalificaties als 'op dit moment' en 'zoals de situatie er nu voor staat'.

9. **Zorg na het oplossen van het incident voor een evaluatiegesprek met de klant:**
   Bespreek de stappen die ondernomen zijn, wat goed en fout ging, wat jouw bevindingen zijn en wat er gedaan kan worden om in het vervolg een datalek te voorkomen.