FORMIN019-REV02 Intern - Beveiligingsinbreuken en incidenten en registreren van afwijkingen

Intern lek of incident:

Deze maatregelen gelden indien er een datalek heeft voorgedaan bij Van Hulten Automatisering B.V./Van Hulten Software B.V. en er (mogelijk) persoonsgegevens zijn gelekt.

VOORBEREIDING

- **Check de samenstelling van het 'crisisteam':** met in elk geval directie, hoofd systeembeheer en eventueel kantoor verantwoordelijke
- **Zorg voor een crisisplan:** Bereid scenario's (voor ISO 27001 form), zorg voor juiste contactgegevens, gebruik templates voor datalek
- **Benoem alle mogelijke doelgroepen:** Stel op voorhand een lijst met communicatiedoelgroepen op; Klanten en prospects, werknemers, klantenservice, dienstverleners en andere partners, toezichthouders
- **Identificeer belangrijke leveranciers**

STAP 1 REAGEER ACCURAAT EN SNEL

- **Meld een datalek of incident zo snel mogelijk aan de betrokkenen, ook al zijn nog niet alle details bekend:** Vertel wat je weet, wat jij en anderen kunnen zien en geef aan wat je gaat doen. Je kunt hiervoor gebruik maken van het template "FORMEX006-REV01 Brief klant betreft incident of datalek bij Van Hulten"
- **Geef een tijdsindicatie:** 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 jullie met een update komen.
- **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'.
- **Indien op grotere schaal een lek; richt je helpdesk hiervoor in:** Zorg dat alle mensen aan de telefoon de details weten en publiceer relevante informatie op je website

STAP 2 WEES OPEN EN EERLIJK

- **Breng het nieuws feitelijk en simpel** en geef aan hoe je de betrokkenen op de hoogte brengt en houdt.
- **Vermijd onvoorwaardelijke uitspraken:** Informatie over de omvang van een datalek is veelal niet meteen voor handen, vermijd daarom onvoorwaardelijke en absolute uitspraken (!)
- **Wees zo compleet mogelijk:** Betrokkenen willen de ernst van een incident kunnen inschatten. Probeer daarom zo goed mogelijk een indicatie te geven van de omvang van een lek of incident.

STAP 3 NEEM VERANTWOORDING

- **Accepteer de verantwoordelijkheid:** zelfs als er sprake is van een misdaad.
- **Vermijd voorwaardelijke excuses:** Excuses aanbieden is cruciaal in het nemen van verantwoordelijkheid. Vermijd voorwaardelijke excuses als 'Wij geloven dat deze inbreuk geen negatieve gevolgen heeft gehad voor onze gebruikers, maar willen ons toch verontschuldigen voor eventuele ongemakken'. Maak alleen excuses als bijvoorbeeld 'we kunnen helaas nog niet meer vertellen, maar hopen dat zo snel mogelijk wel te kunnen, excuus daarvoor'.
- **Als je klant geen schuld heeft aan het incident/datalek;** benadruk dat je klant niet aansprakelijk is voor eventuele schade die voortvloeit uit het lek.

STAP 4 REGEL JE (MEDIA)WOORDVOERING EN -MONITORING

- **Geef het incident een gezicht: Benoem een woordvoerder**: Dat kan afhankelijk van de aard van het incident een expert van de werkvloer zijn of een lid van de directie.
- **Intern is extern:** Houd er rekening mee dat alle informatie over het datalek die je aan medewerkers en betrokkenen verstrekt, ook bij externen terecht komt. Het is onmogelijk om alle communicatie tussen medewerkers en derden te overzien. Publiceer daarom (bijv. op je website of d.m.v. een nieuwsbrief) een FAQ over de feiten en geef hen de contact-gegevens van de klantenservice waar zij naar kunnen doorverwijzen. Vermijd discussie, benoem en ontkracht onjuistheden, verwijs naar relevante online bronnen, bijvoorbeeld je eigen website. Ook hiervoor geld: wie zich goed voorbereid en hier op traint, voorkomt tijdverlies en verwarring op het moment dat je dat niet kunt gebruiken.
- **Blijf actueel en tijdig communiceren:** Blijf tijdig en eventueel op afgesproken tijdstippen met updates te komen.
- **Eindbepaling en afwerking:** Een crisis is tijdelijk en heeft veel impact op de organisatie. Bepaal met het crisisteam wanneer de crisis voorbij is, en wanneer kan worden overgegaan tot de orde van de dag. Vanaf dat moment verloopt alle informatie en communicatie weer via de gangbare kanalen. Sluit met het crisisteam af en bewaar de belangrijkste leermomenten.

LET OP: LOG ALLES; notuleer bij alle vergaderingen/overleg!