DATA DRIVEN MARKETING ASSOCIATION

COMMUNICATIE TIPS BIJ DATALEKKEN

APRIL 2019

DDMA HOW-TO

3 STAPPEN, 5 TIPS BIJ DE MELDPLICHT DATALEKKEN

Op 1 januari 2016 kreeg Nederland een wettelijke meldplicht datalekken. Als er bij een datalek een risico is voor consumenten moet het datalek gemeld worden bij de Autoriteit Persoonsgegevens. Bij datalekken met een hoog risico ben je als organisatie verplicht de personen in het bestand hiervan op de hoogte stellen.

Van een datalek met hoog risico is sprake wanneer er risico is op datamisbruik en -fraude. Denk daarbij aan het lekken van financiële data, inloggegevens, BSN-achtige gegevens, of gegevens die kunnen leiden tot discriminatie of uitsluiting, zoals informatie over verslavingen, seksuele voorkeur, ras, levensovertuiging of gezondheid. De kans op misbruik is sneller aanwezig als het om een grote dataset gaat, dus als je veel gegevens per persoon verzamelt, of gegevens van veel personen.

Om te beoordelen of een datalek gemeld moet worden kun je gebruikmaken van het DDMA stroomschema datalekken. Daarmee kun je besluiten of het aan de toezichthouder en/of de betrokkenen gemeld moet worden.

Hoe een organisatie haar klant of donateur over een datalek informeert kan consumentenvertrouwen en reputatie schaden of verstevigen. Zorg daarom dat je als organisatie bent voorbereid:

- Om te voldoen aan de wettelijke informatieverplichting aan de betreffende personen
- Op aandacht van de media. Data en privacy zijn onderwerpen die in een brede belangstelling staan. Wees voorbereid om vragen van de media en op sociale media op te vangen.

Hoe je dat doet, lees je verder in deze DDMA How-to.

DDMA HOW-TO

5 TIPS BIJ DE MELDPLICHT DATALEKKEN

1 WEES VOORBEREID

- Check de samenstelling van het crisisteam. Zorg dat daarin ten minste één iemand betrokken is uit de directie, IT, legal en marketingcommunicatie. Crisiscommunicatie is een 'operationeel proces', dat vergelijkbaar is met de andere processen in je organisatie.
- Zorg voor een crisisplan. Bereid scenario´s voor, zorg voor contactgegevens van relevante werknemers en standaardteksten voor meldingen aan betrokkenen en media. Train op de uitvoering van het plan.
- Benoem alle mogelijke doelgroepen. Stel op voorhand een lijst met communicatiedoelgroepen op. Klanten en prospects, werknemers, klantenservice, dienstverleners en andere partners, toezichthouders en politiek.
- Identificeer belangrijke leveranciers waaronder externe IT-specialisten, dienstverleners die kunnen assisteren bij de klantenservice, zoals callcenters, en eventueel externe PR- of communicatiespecialisten.

2 REAGEER ACCURAAT EN SNEL

- Meld een datalek zo binnen 72 uur na het vaststellen, 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 bij de toezichthouder gebruik maken van de voorlopige melding, deze kan worden ingetrokken als later blijkt dat melden niet nodig was.
- 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'.
- Richt je klantenservice in. Zorg indien mogelijk voor een gratis telefoonnummer en publiceer relevante informatie op het internet.

3 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 volledig 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. Het doel van de meldplicht is om betrokkenen in staat te stellen om zelf maatregelen te nemen, zoals het blokkeren van creditcards of het afschermen van informatie. Zorg dat betrokkenen de informatie krijgen die nodig is om deze maatregelen te nemen.

4 NEEM VERANTWOORDING

- Accepteer de verantwoordelijkheid, zelfs als er sprake is van een misdrijf.
- 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'.

5 REGEL JE MEDIAWOORDVOERING 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 een FAQ over de feiten en geef hen de contact-gegevens van de klantenservice waar zij naar kunnen doorverwijzen.
- Blijf actueel en tijdig communiceren. Blijf tijdig en eventueel op afgesproken tijdstippen met updates te komen.

- Monitor social media. Introduceer eventueel zelf een hashtag op Twitter, vermijd discussie, benoem en ontkracht onjuistheden, verwijs naar relevante online bronnen, bijvoorbeeld je eigen website. Ook hiervoor geldt: wie zich goed voorbereid en hier op traint, voorkomt tijdverlies en verwarring op het moment dat je dat niet kunt gebruiken.

Tot slot. 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.

VOORBEELDBRIEF

MELDING DATLEK AAN BETROKKENEN

Geachte,

Onze organisatie heeft ontdekt dat een ongeautoriseerde partij zich tussen <datum> en <datum> toegang heeft verschaft tot onze systemen. Zoals het er nu naar uitziet hebben de indringers toegang gehad tot <omschrijving databases en functies>. Hierbij is mogelijk persoonlijke informatie van u gecompromitteerd.

Het gaat hierbij om de volgende gegevens <omschrijving categorieën persoons- gegevens>. In reactie op deze inbreuk hebben wij de volgende stappen ondernomen:

1. Een extern erkende beveiligingsspecialist ingeschakeld om het lek grondig te onderzoeken en aanbevelingen te doen voor verbeteringen in de databeveiliging.
2. De betreffende dienst tijdelijk offline gehaald/ accounts op non actief gesteld/ gecompromitteerde bestanden geïsoleerd.
3. Melding gemaakt van het lek bij de wettelijke toezichthouder: de Autoriteit persoonsgegevens.

Op dit moment onderzoeken wij (samen met eventuele derde IT specialist) welke gegevens uit de systemen zijn ingezien of gedownload. Wij zullen u hierover zo snel mogelijk uitsluitsel geven. Wij geven u vandaag om <tijdstip> in ieder geval een nieuwe update over de stand van zaken.

Wij adviseren u in de tussentijd preventief de volgende stappen te ondernemen:

- Wijzig uw wachtwoord. U kunt dit eenvoudig doen via deze link.
- Indien u voor andere diensten gebruik maakt van hetzelfde wachtwoord, adviseren wij u ook deze wachtwoorden opnieuw in te stellen.

Wij betreuren deze inbreuk zeer en bieden onze excuses aan voor het ongemak dat dit voor u met zich meebrengt. Mocht u vragen hebben naar aanleiding van deze mededeling, neemt u dan contact op met de klantenservice via <(gratis) telefoonnummer> of bekijk de website.

Groet,