Leren van de boete voor Booking.com

Recent publiceerde de Autoriteit Persoonsgegevens het boetebesluit over Booking.com. Dat ging over een lek uit 2019. Al even geleden, maar het besluit va de AP bevat een belangrijke les.

De AP legt 475.000 euro boete op voor 22 dagen te laat melden dat onbevoegden toegang hadden gekregen tot hotelreserveringsgegevens van ca 4.000 personen, zowel afkomstig uit de EU als daarbuiten, waaronder 300 keer inclusief creditcardgegevens.

Zie: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_boete_booking.pdf

Uit dit besluit blijkt het belang om security incidenten meteen te melden in je organisatie. Niet alleen bij de CISO, maar ook bij de FG. De AP kijkt heel streng en formeel naar naleving van de 72-uurseis waarbinnen een datalek gemeld moet worden.

De overtreding bij Booking.com wordt door de AP als ernstig betiteld, ondanks dat het om minder dan 10.000 personen ging, niet om identiteitsbewijzen of BSN's, er géén bijzondere persoonsgegevens toegankelijk waren, de e-mailadressen van de hotelklanten niet leesbaar waren (want gehasht) en Booking.com zelf bij de AP heeft gemeld op het moment dat de security afdeling had vastgesteld dat er inderdaad een lek was in een reserveringssysteem. Probleem is dat er dus eerst intern is gekeken of er ook echt een datalek was, met toegang tot persoonsgegevens, of alleen een beveiligingsincident. En de tijd die is genomen voor dat interne onderzoek was dus langer dan de 72 uur.

Wat is de les die we daaruit kunnen trekken? Het is goed om altijd een voorlopige melding te doen, ook al weet je nog niet zeker hoe groot/erg het lek is. Die melding kun je intrekken als uit nader onderzoek blijkt dat er toch géén sprake was van een datalek. Intrekken omdat een melding toch overbodig bleek is geen probleem, maar eerst uitzoeken en daardoor te laat melden dus wel. Zo'n voorlopige melding kun je alleen op tijd indienen als iedereen binnen je organisatie onmiddellijk alert reageert bij een niet pluis

signaal. Klop dus aan bij de CISO en FG. Liever een keertje teveel aan de bel trekken dan achteraf een boete.