Auteur: Peter van Schelven is jurist en arbiter bij BIJ PETER - Wet & Recht en bereikbaar via linkedin.com/in/petervanschelven. Bianca Brooijmans is FG bij Enovation Group en zelfstandige. Bianca is bereikbaar via linkedin.com/in/biancabrooijmans.

‘Mind your step’: wat leert de AP-boete van Transavia ons?

Afgelopen november publiceerde de Autoriteit Persoonsgegevens (AP) het besluit waarmee Transavia een bestuurlijke boete van 400.000 euro is opgelegd. De toezichthouder kwam tot die sanctie vanwege een ondermaatse beveiliging van persoonsgegevens. Het boetebesluit van de AP is de moeite van het lezen waard omdat het uitvoerig ingaat op het onderwerp van de toegang tot IT-systemen.

In de herfst van 2019 bleek dat een hacker zich onbevoegd toegang tot de IT-systemen van de luchtvaartmaatschappij te hebben verschaft, waardoor gegevens van zo’n 80.000 passagiers, 3.000 medewerkers en 200 leveranciers konden worden bemachtigd. Daar zaten onder andere BSN-nummers en gezondheidsgegevens van passagiers, bijvoorbeeld over rolstoelgebruik, tussen. Kortom, een fors datalek.

De melding van het datalek vormde de opstap voor onderzoek van de AP, die begrijpelijkerwijs concludeerde dat de Algemene Verordening Gegevensbescherming (AVG) was overtreden. Het onderzoek maakte duidelijk dat de hacker gebruik had gemaakt van een aanval door middel van ‘password spray’ en ‘credential stuffing’. Van ‘password spray’ is sprake als veelgebruikte wachtwoorden op een geautomatiseerde wijze worden ingezet om toegang tot IT-systemen te krijgen. Bij ‘credential stuffing’ gebruikt een hacker, uit andere datalekken, van derden afkomstige gebruikersgegevens. Eenmaal bij Transavia binnen deed de hacker in kwestie zich voor als vertrouwde gebruiker met de hoogste privileges in het systeem.

Nadere concretisering van securitynorm

Artikel 32 van de AVG, de algemeen geformuleerde bepaling over de verplichting tot beveiliging van persoonsgegevens, geeft niet concreet aan hoe en met welke middelen een organisatie de toegang tot haar IT-systemen moet inrichten. De AVG zegt wel dat je als organisatie ‘passende technische en organisatorische maatregelen’ moet nemen die een, op het risico afgestemd, beveiligingsniveau waarborgen. Al met al een tamelijk vage norm. Met name de openheid van deze wettelijke regel roept in de praktijk meer dan eens de vraag op of je als organisatie wel voldoende security in huis hebt om compliant te zijn met de AVG. Het boetebesluit inzake Transavia helpt ons wat die vraag betreft wel een klein stapje verder. De Autoriteit Persoonsgegevens zegt onder meer het volgende: ‘De maatregelen die Transavia had kunnen nemen ten tijde van de inbreuk, waren reeds een norm volgens Transavia zelf, volgens leveranciers en volgens internationale standaarden. Verder bleek dat er bepaalde maatregelen wel al deels waren geïmplementeerd door Transavia.’

Het opmerkelijke van dit citaat is dat de AP, bij de beantwoording

van de vraag welke securitymaatregelen zij onder de AVG geboden acht, niet alleen uitgaat van min of meer objectieve maatstaven, zoals de welbekende securitystandaarden, bijvoorbeeld ISO27001. Volgens die standaarden moeten, naar wij bekend veronderstellen, toegangsrechten worden beperkt en gecontroleerd. Maar de AP gaat in haar aanpak een behoorlijke stap verder. Zij doet namelijk voorkomen dat die aanpak past in de toepassing van artikel 32 AVG. Want wat doet de toezichthouder? In zekere zin subjectiveert zij de wettelijke securityverplichting door uitdrukkelijk aan te knopen bij dat wat in de ogen van Transavia zélf, zo blijkt uit haar eigen securitydocumenten, relevante maatregelen zijn. Anders gezegd: de regels van het IT-securityrecht komen niet alleen van buiten en zijn niet louter een extern gegeven, maar is ook iets wat je als organisatie zelf inhoud geeft. Een voor de hand liggende insteek nu de securityregels van de AVG meer vragen dan antwoorden opwerpen. De set van spelregels onder de AVG voor wat betreft informatiebeveiliging wordt door het eigen gedrag van de organisatie ingevuld. Securityrecht is geen 'law in the books', maar 'law in action'. Het boetebesluit lezende maakt het ons dan ook duidelijk dat de AP Transavia (mede) heeft afgerekend op de inhoud van haar eigen securitybeleidsdocumenten en de gebrekkige wijze waarop het luchtvaartbedrijf aan die documenten uitvoering heeft gegeven. Dat gaat dus aanzienlijk verder dan louter een toets aan de tekst van de AVG en de gangbare securitystandaarden.

Een voorbeeld: wachtwoordbeleid

Transavia beschikte over een uitvoerig uitgewerkt wachtwoordbeleid. Daarin was aangegeven welke eisen er golden per gebruiker en per mogelijk risiconiveau. Hoe hoger het risiconiveau, des te zwaarder de eisen voor een wachtwoord. Het bedrijf onderscheidde wachtwoorden met een standaard risiconiveau, wachtwoorden met additionele maatregelen voor gebruikers met meer bevoegdheden en tevens wachtwoorden voor 'hoog risico gebruikers'. In de beleidsdocumenten was ook het gebruikelijke onderscheid gemaakt tussen 'generieke accounts' en aan individuele gebruikers gekoppelde 'user accounts'. In haar onderzoek heeft de AP Transavia gevraagd waarom de generieke accounts die betrokken waren bij de hack niet voldeden aan het eigen wachtwoordenbeleid. De luchtvaartmaatschappij heeft daarop geantwoord dat haar focus vooral lag op user accounts, enerzijds omdat dat meer accounts betrof en anderzijds omdat zij meende dat bij die accounts de meeste risico's zouden liggen. Transavia stelde zich op het standpunt dat de kans op een succesvolle 'password spray'-aanval of 'credential stuffing attack'-groter was bij user accounts dan bij generieke accounts. De AP gaat daaraan volledig voorbij. Zij maakt met het antwoord korte metten: "De wachtwoorden van de gecompromitteerde accounts voldeden niet aan het eigen beleid en waren in die zin niet passend voor het beoogde niveau van beveiliging."

Zie hier de dus insteek van de AP:

- Het 'eigen beleid' van Transavia blijkt voor de AP een wezenlijk vertrekpunt te zijn bij het bepalen van de reikwijdte van de securityverplichting. Zo krijgt het eigen securitybeleid in zekere zin een juridische lading.
- Niet de vraag of, zoals de AVG verlangt, Transavia voorziet in 'passende' security-maatregelen staat voorop, maar wel of de getroffen securitymaatregelen passend zijn voor het door Transavia zélf 'beoogde' niveau van security. Het eigen beleid is dus 'leading' in de beoordeling van de vraag of de AVG geschonden is.

Slot

Het boetebesluit van de AP lijkt ons op zich niet onredelijk; de informatiebeveiliging van Transavia zoals aanwezig in najaar 2019 kon de toets der kritiek eenvoudigweg niet doorstaan. Maar meer specifiek leert het boetebesluit ons ook dat de AP bij een security-onderzoek naar aanleiding van een datalek een klassiek-juridische 'truc' toepast: confronteer de organisatie met haar eigen woorden. Dus: kijk naar dat wat de eigen beleidsdocumenten van de organisatie zeggen en geef die documenten vervolgens een prominente plek bij het bepalen van de vraag of een organisatie de securityverplichting van de AVG wel of niet naar behoren heeft nageleefd. Zoals gezegd: niet alleen de tekst van de AVG en de algemeen aanvaarde beveiligingsstandaarden (bijv. van ISO en NEN) geven inhoud aan het securityrecht, ook het eigen securitybeleid van de organisatie vormt een bron voor de beoordeling. De AP betrekt in de beoordeling of je je eigen woorden als organisatie serieus hebt genomen. Is dat niet het geval, dan maak je de AP het makkelijk om jouw organisatie daarop af te rekenen. Grof gezegd: opgeknoopt aan je eigen woorden…

Dit alles gezegd hebbende, is securitybeleid onmiskenbaar meer dan alleen 'een' securitybeleid. Je maakt er eigen normen mee waar de AP op kan terugvallen. Houd dat voor ogen wanneer je je als security- of privacy professional buigt over het maken of beoordelen van een securitybeleidsdocument. 'Mind your step...'

Referentie

(1) Besluit Autoriteit Persoonsgegevens 23 september 2021 t.a.v. Transavia Airlines C.V, gepubliceerd 12 november 2021.