10 lessen uit uitspraken van de Autoriteit Persoonsgegevens

ZO ZORG JE VOOR PASSENDE INFORMATIE-BEVEILIGING

SYSTEMEN EN DATA MOETEN 'PASSEND' WORDEN BEVEILIGD, STAAT STEEDS VAKER IN WET- EN REGELGEVING. WAT BETEKENT DAT VOOR ORGANISATIES? WANNEER IS INFORMATIEBEVEILIGING PASSEND TE NOEMEN? AAN DE HAND VAN SANCTIEBESLUITEN VAN DE AUTORITEIT PERSOONSGEGEVENS BELICHTEN JEROEN VAN HELDEN EN MICHELLE WIJNANT TIEN BELANGRIJKE AANDACHTSPUNTEN.

door Jeroen van Helden en Michelle Wijnant beeld Shutterstock

VIA PASSWORD SPRAYING KREEG EEN HACKER TOEGANG TOT HET BEDRIJFSNETWERK VAN TRANSAVIA

De tijd dat het domein van informatiebeveiliging enkel iets was voor IT'ers, is voorbij. Steeds vaker is in wet- en regelgeving de verplichting opgenomen om systemen en data te beveiligen. Nalatigheid kan resulteren in civielrechtelijke aansprakelijkheid of sancties van toezichthouders. Met de voorgestelde NIS2-richtlijn komt ook bestuurdersaansprakelijkheid nadrukkelijk in het vizier. Het is daarom belangrijker dan ooit dat IT'ers basiskennis hebben van risicomanagement en het relevante juridisch kader en dat juristen ten minste een redelijk begrip hebben van het vakgebied informatiebeveiliging. Dit artikel poogt

aan die kruisbestuiving een bijdrage te leveren.
Op grond van de Algemene verordening gegevensbescherming (AVG) moet iedere organisatie technische en organisatorische maatregelen nemen om informatiesystemen die persoonsgegevens verwerken, 'passend' te beveiligen. Hierbij moet de organisatie rekening houden met de stand van de techniek, de uitvoeringskosten, de risico's voor betrokkenen en met de aard, de omvang, de context en de verwerkingsdoeleinden. Kort samengevat: hoe gevoeliger en omvangrijker de data, hoe strenger de eisen; hoe goedkoper en gebruikelijker een maatregel, hoe eerder deze moet worden toegepast. De afgelopen jaren legde de Autoriteit Persoonsgegevens (AP) ten minste tien administratieve boetes of dwangsommen op, in een paar gevallen zelfs allebei, wegens gebrekkige informatiebeveiliging. Voor geen enkele andere AVG-verplichting werden door de AP zoveel sancties opgelegd. Dit onderstreept het centrale belang van de beveiligingsverplichting.

TIEN AANDACHTSPUNTEN

Aan de hand van deze sanctiebesluiten brengen we tien aandachtspunten onder de aandacht, voor het realiseren van een passende informatiebeveiliging. Voor iedere securityexpert zijn deze aandachtspunten vermoedelijk redelijk voor de hand liggend, maar dit maakt ze vanuit juridisch oogpunt niet minder belangrijk. Dit zijn immers de aspecten waar de AP als eerste oog voor heeft bij de beoordeling van de kwaliteit van de informatiebeveiliging binnen een organisatie. Het is het 'laaghangend fruit' waar iedere organisatie minimaal aan zou moeten voldoen.
Voor de gemiddelde IT'er ligt de nadruk die door de AP wordt gelegd op documentatie en verantwoording misschien minder voor de hand. Een voorname oorzaak is het feit dat organisaties op grond van de AVG aantoonbaar moeten voldoen aan hun verplichtingen. Zonder adequaat beleid dat is vastgesteld op managementniveau is het lastig om aan dit aspect van de AVG te voldoen. Compliance alleen is dus niet voldoende, een organisatie moet inzichtelijk kunnen maken hoe compliance procesmatig is vormgegeven.

1. RISICOANALYSE

Een organisatie moet beveiligingsmaatregelen treffen op basis van een risicoanalyse. Dit doet een organisatie door dreigingen te inventariseren die kunnen leiden tot een incident, de gevolgen die het incident kan hebben voor betrokkenen en de kans dat de dreiging zich voordoet. Deze analyse moet bovendien worden ingebed in een Plan-Do-Act-Check-cyclus. Het is aan de organisatie om aan te tonen dat zo'n risicoanalyse daadwerkelijk is uitgevoerd. In de UWV-casus oordeelt de AP dat het UWV de risico's voor werkzoekenden

AUTEUR

JEROEN VAN HELDEN
is advocaat IT, IE & Privacy bij De Clercq Advocaten Notariaat. Hij adviseert en procedeert op het gebied van (internationale) privacy en dataprotectie-vraagstukken en IT-projecten.

AUTEUR

MICHELLE WIJNANT
is advocaat IT, IE & Privacy bij De Clercq Advocaten Notariaat. Ze adviseert en ondersteunt onder meer CISO's en FG's bij de uitvoering van hun werkzaamheden.

#	Datum	Overtreder	Boete (€)	Dwangsom (€)
1	24 februari 2022	Ministerie van Buitenlandse Zaken	565.000	800.000
2	23 september 2021	Transavia	400.000	-
3	31 mei 2021	UWV	450.000	-
4	4 februari 2021	Orthodontiepraktijk	12.000	-
5	26 november 2020	OLVG	440.000	-
6	18 juni 2019	HagaZiekenhuis	460.000	300.000
7	31 juli 2018	UWV	-	900.000
8	15 februari 2018	Menzis	-	250.000
9	15 februari 2018	VGZ	-	750.000
10	6 februari 2017	Nationale politie	-	200.000

bij het verzenden van groepsberichten via de 'Mijn Werkmap-omgeving' niet of onvoldoende in kaart heeft gebracht.

2. BEVEILIGINGSPLAN

Iedere organisatie moet beveiligingsbeleid hebben opgesteld, waaronder een beveiligingsplan waarin is vastgelegd welke beveiligingsmaatregelen zijn geïmplementeerd op basis van risicoanalyses. Hoewel het ministerie van Buitenlandse Zaken beschikte over diverse data protection impact assessments (DPIA's) en kwetsbaarheidsanalyses voor een systeem waarmee zij visumaanvragen verwerkte, had zij geen plan waaruit bleek welke concrete beheersmaatregelen zij nu had doorgevoerd. Bij de nationale politie was eveneens geen beveiligingsplan aanwezig.

3. OPLEIDING PERSONEEL

Personeel moet passende trainingen krijgen op het gebied van informatiebeveiliging. Deze trainingen moeten worden gegeven aan medewerkers die pas in dienst zijn (bijvoorbeeld tijdens een on-boarding programma) en aan medewerkers die al langer in dienst zijn. Onderwerpen die aan bod zouden moeten komen, zijn: gebruik van systemen, relevante wet- en regelgeving en beveiliging. Welke trainingen voor medewerkers precies relevant zijn, hangt af van de betreffende functies. Binnenlandse Zaken had dit aspect wel op orde; de nationale politie schoot op dit punt tekort.

4. AUTORISATIEMATRIX

Een organisatie moet beschikken over formeel vastgestelde procedures voor het activeren en afmelden van toegangsrechten tot systemen. Werkinstructies die niet formeel zijn vastgesteld zijn daarvoor onvoldoende, aldus de AP in de BZ-casus.
Ook moet een autorisatiematrix op basis van gebruikersprofielen worden gebruikt, waarin de taken en verantwoordelijkheden van groepen gebruikers duidelijk en gemotiveerd zijn beschreven. Eenmaal verstrekte autorisaties moeten periodiek worden gecontroleerd en, indien nodig, aangepast.

5. STERKE WACHTWOORDEN

Door sterke wachtwoorden toe te passen wordt voorkomen dat een aanvaller toegang krijgt tot systemen door veel gebruikte of eerder gelekte wachtwoorden te proberen. Transavia had weliswaar beleid op dit punt, maar dat werd alleen consequent toegepast en afgedwongen op individuele accounts en niet op generieke accounts. Een hacker kon daardoor via password spraying toegang krijgen tot een generiek account en zo tot het bedrijfsnetwerk.

6. MFA

Sterke wachtwoorden alleen zijn niet altijd voldoende. Soms moet authenticatie plaatsvinden op basis van een extra factor. Volgens de AP is Multi Factor Authentication (MFA) in ieder geval vereist bij inlog op Citrix en andere telewerkomgevingen (Transavia), voor het verkrijgen van toegang tot zorginformatiesystemen (OLVG, HagaZiekenhuis) en voor het verkrijgen van toegang tot ziekteverzuimgegevens (UWV).

7. NETWERKSEGMENTATIE

Met netwerksegmentatie worden de systemen die onderling moeten communiceren in aparte segmenten geplaatst. Gebruikers krijgen alleen toegang tot de segmenten die zij nodig hebben. In de Transavia-casus bleek netwerksegmentatie niet of onvoldoende te zijn toegepast, waardoor de hackers zich relatief gemakkelijk door het netwerk konden bewegen toen zij eenmaal binnen waren.

8. CRYPTOGRAFIE

Waar passend moet een organisatie gebruik maken van versleuteling van persoonsgegevens. Transport Layer Security (TLS) is het meest gebruikte protocol voor het beveiligen van internetverbindingen. Toepassing van TLS op internetverkeer geschiedt via het HTTPS-protocol aan de hand van een TLS-certificaat. Dit certificaat kan kosteloos worden verkregen. De orthodontiepraktijk maakte gebruik van een inschrijvingsformulier op de website zonder gebruik te maken van dit beveiligde protocol, hetgeen resulteerde in een inbreuk op de AVG.

9. LOGGING EN CONTROLE LOGBESTANDEN

Handelingen die gebruikers uitvoeren met persoonsgegevens, zoals raadplegingen en mutaties, moeten worden gelogd (Menzis, VGZ). De logbestanden moeten periodiek worden gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van gegevens. Deze controles moeten proactief, systematisch en consequent plaatsvinden (BZ, HagaZiekenhuis, OLVG). In het geval van een ziekenhuis is het doen van acht incidentele controles en twee proactieve steekproeven in een periode van ruim 15 maanden ruimschoots en evident onvoldoende (OLVG). Zes proactieve steekproeven per jaar is ook niet voldoende, aldus de AP en bevestigd door de rechtbank Den Haag (HagaZiekenhuis).[1] Helaas is niet duidelijk hoeveel steekproeven wel voldoende zou zijn geweest.

10. PROCEDURE DATALEKKEN

Een organisatie moet beschikken over een procedure voor het melden en opvolgen van beveiligingsincidenten en datalekken. BZ beschikte alleen over een procedure voor medewerkers voor het intern melden van datalekken, niet voor de opvolging daarvan. Ook was de procedure niet op managementniveau vastgesteld. Buiten dat de AP boetes heeft opgelegd voor een gebrekkige procedure datalekken, zijn er ook al meerdere boetes opgelegd voor het niet of te laat melden van een datalek. Een deugdelijke procedure datalekken helpt dit te voorkomen.

Bronnen:

[1] Rechtbank Den Haag, 31 maart 2021, ECLI:NL:RBDHA:2021:3090.