PRIVACY 1 | *09 februari 2016*

Datalek wordt boardroom topic

Leestijd van ongeveer 9 minuten 3 reacties

Naar schatting zijn er in januari 2016 enkele tientallen 'datalekken' gemeld bij de Autoriteit Persoonsgegevens. Bij niet melden, kan de boete een materiële post worden. Alleen al daarom dwingt de op 1 januari 2016 ingevoerde meldplicht accountantskantoren en hun cliënten werk te maken van de beveiliging van persoonsgegevens. Een introductie in zes vragen.

1. Wat zijn datalekken?

Volgens de wet kun je spreken van een datalek als er inbreuk wordt gemaakt op de beveiliging, waardoor persoonsgegevens verloren gaan of onrechtmatig worden verwerkt. Je hebt niet alleen een datalek als persoonsgegevens uitlekken, maar ook als die bijvoorbeeld door een computercrash verloren gaan of op de een of andere manier ontoegankelijk worden. Bij dat laatste valt bijvoorbeeld te denken aan hackers die een systeem 'gijzelen' totdat er wordt betaald.

Soms liggen persoonsgegevens letterlijk op straat. Zo liet elf jaar geleden een kapitein van de landmacht een geheugenstick met geheime informatie over de Nederlandse militairen in Afghanistan in een huurauto liggen. Hij kreeg de stick weliswaar terug, maar de 'eerlijke vinders' hadden de gegevens wel eerst gekopieerd.

Het is altijd uitkijken met een usb-stick. Verliezen is één ding. Maar je kunt ook een stick aangereikt krijgen met een leuk filmpje of spelletje, dat *malware* installeert op de laptop of pc. Daarmee kunnen hackers vervolgens via het bedrijfsnetwerk allerlei persoonsgegevens wegsluizen. Bijvoorbeeld informatie over de winstuitkeringen aan partners.

LAATSTE ARTIKELEN

STATISTICAL AUDITING (78) | *22 augustus 2019*
Data-analyse - een poging om de bomen in het bos te zien

FORUM | *19 augustus 2019*
Rel FvD: accountant komt als winnaar uit de bus

DATA SCIENCE | *14 augustus 2019*
'Dit gaat ons vak veranderen'

LEIDERSCHAP | *09 augustus 2019*
Gespreid leiderschap versus positioneel leiderschap binnen accountantskantoren

COLUMN ARBEIDSRECHT | *06 augustus 2019*
Wel of niet 'all-in'?

MEER ARTIKELEN

Hackers zijn lang niet meer alleen romantische zonderlingen die een geslaagde hack als doel op zich zien. Het zijn steeds vaker leden van criminele organisaties die op grote schaal zoeken naar zwakke plekken in systemen. Want die zwakke plekken bieden de mogelijkheid om persoonsgegevens te stelen waarmee ze op andermans naam bestellingen kunnen doen.

'Het zijn steeds vaker criminele organisaties die op grote schaal zoeken naar zwakke plekken in systemen.'

Dat maakte de DigiNotar-hack zo ernstig. Een lek bij een DigiD-leverancier zet immers de deur open naar allerlei gevoelige gegevens. Ook de hack bij AIS Fligth Academy kan lelijke gevolgen hebben gehad. Daar vonden hackers niet alleen de namen en adressen van piloten in opleiding, maar ook paspoortgegevens en informatie over schulden en strafrechtelijke antecedenten.

Datalekken zijn soms veel dichterbij dan je denkt. Werknemers die met hun laptop of smartphones een openbaar netwerk gebruiken in bijvoorbeeld een restaurant of in de trein kunnen een gemakkelijk doelwit zijn voor een hacker. Met een apparaatje van een paar tientjes en een goeie batterij zet die een eigen netwerkje op, dat de argeloze gast of reiziger vervolgens gebruikt om online te betalen of vertrouwelijke gegevens te versturen.

Accountantskantoren en bedrijven hebben vaak een intern netwerk met een gedeelde harde schijf. Ontslagen werknemers - vaak niet de meest loyale - kunnen nog bij alle persoonsgegevens op die schijf zo lang hun inloggegevens niet zijn geblokkeerd. Die blokkade moet dus onderdeel zijn van het HRM-beleid.

Verborgen cc-adressen

Ook geen zeldzaamheid is een mail met niet verborgen cc-adressen. Zo verspreidde de politie Delft in 2009 650 mailadressen van deelnemers aan Burgernet, zodat je precies kon zien wie de 'verklikkers' waren in de buurt. Overigens beging Deloitte twee jaar eerder eenzelfde cc-fout. Een Belgische vestiging moest toezien op een zorgvuldig verloop van de aanvraagprocedure van een numeriek .nl-domein. Het verstuurde in een *reply to all* de mededeling dat 'meerdere deelnemers' de aanvraagvergoeding nog niet hadden betaald. Veel deelnemers verloren door dit lek het vertrouwen in de bewaker van de zorgvuldigheid.

Ook bedrijven die elektronisch communiceren met klanten via een contactformulier op de website of nieuwsbriefabonnees dan wel eventdeelnemers werven via een online inschrijfformulier hebben een potentieel lek.

2. Wat doe je ertegen?

Het gebruik van online contactformulieren of inschrijfformulieren is gemakkelijk te beveiligen. Je moet ervoor zorgen dat de klant, de abonnee of deelnemer zijn persoonsgegevens versleuteld kan versturen. In veel gevallen is een site met een beveiligde verbinding te herkennen aan een groen slotje vóór en https:// aan het begin van het webadres. Zie bijvoorbeeld de adresbalk boven dit artikel. Ook het versleutelen van de gegevens op informatiedragers kan een hoop ellende besparen. Omdat de gevolgen van een datalek bij goede encryptie beperkt blijven, hoef je het datalek niet aan de betrokkenen te melden als de gegevens voldoende versleuteld zijn. (*Maar wel aan de Autoriteit Persoonsgegevens, zie hieronder.*)

DigiD-leverancier DigiNotar liet na de inbraak onderzoek doen, maar zag een belangrijk deel van het lek over het hoofd en ondernam daar niets tegen. Toen er bij nader inzien 247 nepcertificaten in omloop waren, zegden Microsoft, Google Chrome en Mozilla het vertrouwen in de DigiNotar-certificaten op. Het bedrijf ging failliet en de oprichters moesten de eigenaar zijn geld terugbetalen.

'Het gebruik van online contactformulieren of inschrijfformulieren is gemakkelijk te beveiligen.'

Je moet kortom beleid op papier zetten en maatregelen nemen om datalekken te voorkomen en te herstellen. Herman Braam van Privyon, die onder meer de NBA adviseert over beveiliging van persoonsgegevens, deed eens onderzoek bij een koepelorganisatie van advocatenkantoren. Slechts enkele kantoren bleken hun zaakjes op orde te hebben. In zo'n geval is een eerste stap iemand aanwijzen die verantwoordelijk is en een team formeren dat onder meer de kwetsbaarheden in de organisatie in kaart brengt.

Een zwak punt is altijd oude software, waarvoor geen updates en fixes meer worden geleverd, zo weten ze in Het Groene Hart Ziekenhuis. Daar hadden hackers toegang tot onder andere de burgerservicenummers van 493 duizend patiënten, onder wie bekende Nederlanders. Een beveiligingsbedrijf ontdekte de inbraak en waarschuwde. De directie kwam echter pas in actie nadat de hacker de pers had ingelicht. De software werd vernieuwd en het systeem is nu zo gecompartimenteerd dat je van de achterdeur niet meer helemaal kunt doorlopen naar de zolder.

'Een eerste stap is iemand aanwijzen die verantwoordelijk is.'

De hospitaal-hack laat zien dat de techniek veel kan oplossen, maar dat de mens vaak de zwakste schakel is. Daarom moet het personeel een zeker privacyrisicobewustzijn worden bijgebracht.
Die noodzaak blijkt ook uit een hack bij de Amerikaanse winkelketen Target in 2013. Daar rinkelden de bellen van het beveiligingssysteem zo vaak, dat de werknemers er horendol van werden en niet opletten toen er echt iets aan de hand was. In vier maanden tijd maakten hackers onder meer de beveiligings- en pincodes van meer dan 40 miljoen credit cards buit. Dat je de effectiviteit van de privacymaatregelen volgens de Wet bescherming persoonsgegevens moet blijven controleren, is tegen deze achtergrond logisch.

3. Wanneer moet je melden?

'De mens is vaak de zwakste schakel. Daarom moet het personeel privacyrisicobewustzijn worden bijgebracht.'

Dat hangt van de ernst van het lek af. Je moet een lek binnen 72 uur melden bij de Autoriteit Persoonsgegevens als het leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens of als er een 'aanzienlijke kans' op ernstig nadeel is. De ernst hangt niet alleen samen met het aantal gegevens dat verloren is gegaan, maar ook van de gevoeligheid van die gegevens.

Gevoelige gegevens zijn persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid en seksuele leven. Gevoelig zijn ook gegevens over:

- salarissen;
- betalingsgegevens;
- lidmaatschap van een vakvereniging;
- opgelegd straffen of sancties;
- (problematische) schulden;
- gokverslaving;

- prestaties op school of werk;
- relatieproblemen.

Verder moet je datalekken melden als het gaat om gegevens, waarmee onverlaten (identiteits)fraude kunnen plegen, zoals biometrische gegevens, kopieën van identiteitsbewijzen en burgerservicenummers. Fraude en misbruik liggen uiteraard ook op de loer bij het verlies van:

- gebruikersnamen;
- wachtwoorden;
- andere inloggegevens.

Het verlies van inloggegevens ligt extra gevoelig, omdat gebruikersnamen en wachtwoorden vaak ook op andere plekken worden gebruikt. Zo kan het wachtwoord voor een winkelsite hetzelfde zijn als dat voor internetbankieren. Als het lek 'waarschijnlijk ongunstige gevolgen' zal hebben voor de betrokkene moet de verantwoordelijke de lekkage niet alleen melden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene zelf.

4. Wat gebeurt er als je meldt?

De Autoriteit Persoonsgegevens zal volgens voorzitter Jacob Kohnstamm een onderzoek instellen als zij vermoedt dat er meer aan de hand is. Maar de toezichthouder hoeft niet alle meldingen te onderzoeken. In eerste instantie is de bedoeling van de meldplicht namelijk vooral dat verantwoordelijken zorgvuldiger omgaan met persoonsgegevens.

De toezichthouder zal een 'bindende aanwijzing' geven aan de melder als die onvoldoende maatregelen heeft genomen om het datalek te dichten en nieuwe datalekken te voorkomen. De verantwoordelijke krijgt een bepaalde termijn om die aanwijzing op te volgen.

De toezichthouder publiceert de meldingen niet en nagelt melders evenmin aan de schandpaal. Op basis van een reeks meldingen kan de Autoriteit Persoonsgegevens wel informatie naar buiten brengen 'op geaggregeerd niveau'. Bijvoorbeeld om het publiek in zijn algmeenheid te waarschuwen voor bepaalde risico's.

5. Wat gebeurt er als je niet meldt?

Je kunt natuurlijk proberen het lek in alle stilte te dichten en doen alsof er niets aan de hand was. Maar in dit informatietijdperk blijft een lek niet lang verborgen. Al was het maar omdat iemand de Autoriteit Persoonsgegevens tipt.

Als je wel een melding doet aan de Autoriteit Persoonsgegevens, maar ten onrechte niet de betrokkenen inlicht, kan de autoriteit dat alsnog opdragen.

'Het College Bescherming Persoonsgegevens kan forse boetes opleggen tot maximaal tien procent van de jaaromzet.'

Tot 2016 was de toezichthouder een papieren tijger, die maximaal 4.500 euro boete kon opleggen als organisaties niet meldden dat zij persoonsgegevens verwerkten. Maar het College Bescherming Persoonsgegevens is nu een autoriteit, die net als bijvoorbeeld de AFM, forse boetes kan opleggen voor allerlei overtredingen van de privacywetgeving.

Voor de hoogte van de boete gelden verschillende bandbreedtes. Het maximum in de hoogste categorie is 820 duizend euro. De boete gaat omlaag als je goed meewerkt aan het onderzoek van de toezichthouder, uit eigen beweging het lek dicht, een wetsovertreding meldt/beëindigt en/of de schade vergoedt aan de gedupeerden. Voor recidivisten gaat de boete met vijftig procent omhoog.

Als een organisatie een bindende aanwijzing niet opvolgt en de autoriteit de maximale boete daarvoor een lachertje vindt ('als onvoldoende bestraffend wordt ervaren'), kan zij de boete verhogen tot maximaal tien procent van de jaaromzet. Maar dan moet het wel gaan om ernstige schendingen als ongeoorloofde handel in persoonsgegevens of het botweg negeren van bindende aanwijzingen bij substantiële wetsovertredingen. Bij niet-melden zal het zo'n vaart niet lopen.

6. In control

'Je moet als verantwoordelijke kunnen aantonen dat je in control bent. En dat moet je continu monitoren.'

Herman Braam van Privyon. "Je moet als verantwoordelijke kunnen aantonen dat je *in control* bent. En dat moet je continu monitoren. Je ziet nu dat privacy veel meer een *boardroom topic* is geworden. Een datalek kan niet alleen leiden tot reputatieschade, maar kan ook materiële gevolgen hebben. Een boete tot tien procent van de jaaromzet kan een materiële post zijn."

Boetes zijn echter niet de enige kostenpost bij datalekken. Je moet immers alsnog allerlei maatregelen treffen om de aangerichte schade te herstellen en toekomstige schade te voorkomen. Koen Versmissen, adviseur bij Privacy Management Partners en coauteur van *Grip op Datalekken*. "Een lek kost zo'n 150 tot 200 euro per persoon. Bij omvangrijke bestanden lopen de kosten dus flink op."

Meer informatie

- www.autoriteitpersoonsgegevens.nl
- www.privyon.nl
- https://www.accountant.nl/nieuws/2016/2/gbned-rapport-over-meldplicht-datalekken-en-privacy-shield/

Enkele voorbeelden zijn ontleend aan het boek van Koen Versmissen e.a.,
zie www.gripopdatalekken.nl.

Lex van Almelo
Journalist en juridisch medewerker van Accountant/Accountant.nl.
Lees alles van Lex van Almelo

NIEUWS | *16 augustus 2019*

Merendeel accountantskantoren voldoet niet geheel aan AVG

Nog lang niet alle accountantskantoren voldoen volledig aan de AVG. Hoewel informatiebeveiliging meer aandacht krijgt, blijkt er nog veel ruimte te zijn voor verbetering. →

x 6

OPINIE | *07 augustus 2019*

Privacy: de Belastingdienst als nieuwe Facebook?

De Belastingdienst is regelmatig in het nieuws met privacy-schendingen. Al weer jaren geleden kreeg de dienst van de Hoge Raad een tik op de vingers, over het verzamelen van kentekenplaatgegevens van auto's. →

x 2 **52** **34**

Annabel Vissers en Vincent Leenders

NIEUWS | *24 juli 2019*

Facebook krijgt privacyboete van vijf miljard

Facebook betaalt de Amerikaanse marktwaakhond FTC een boete van vijf miljard dollar wegens verschillende privacyschandalen. Het gaat om de hoogste schikking die de toezichthouder ooit trof met een bedrijf. Ook wordt Facebook verplicht een onafhankelijke commissie in te stellen voor privacyzaken. →

x 0

NIEUWS | *11 juli 2019*

RSM: '270.000 eigenaren van familiebedrijven dreigen privacy te verliezen'

Vanaf januari 2020 zijn ondernemingen en rechtspersonen verplicht om hun (in)directe eigenaren te registreren. Dit leidt tot privacyproblemen voor eigenaren van familiebedrijven. →

x 2

NIEUWS | *23 mei 2019*

'Nog steeds problemen met privacywet AVG'

Veel bedrijven kampen bijna een jaar na invoering van de nieuwe Europese privacyregels in de Algemene Verordening Gegevensbescherming (AVG, of GDPR in het Engels) nog met problemen met de uitvoering van de richtlijn. →

x 3

Aanmelden nieuwsbrief

Ontvang elke werkdag (maandag t/m vrijdag) de laatste nieuwsberichten, opinies en artikelen in uw mailbox.

Bent u NBA-lid? Dan kunt u zich ook aanmelden via uw ledenprofiel op MijnNBA.nl.

Upgrade naar een ondersteunde browser om een reCAPTCHA-uitdaging te ontvangen.

Waarom gebeurt dit?

Privacy - Voorwaarden

Uw e-mail adres

Aanmelden

Accountant is een uitgave van de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA).

NBA

ACCOUNTANT.NL

Home
Nieuws
Opinie
Carrière
Feiten en cijfers
Artikelen

THEMA'S

Aansprakelijkheid
Arbeidsrecht
Corporate governance
Externe verslaggeving
Fiscaal
Fraude in praktijk
Kantoormanagement
Mkb
Opleiding
Privacy
Samenstellen
Statistical auditing
Accountantsdag
Assurance
Dag van de Financial
Financiële instellingen
Flex-bv
ICT
Kwaliteit en toezicht
Ondernemingsrecht
Overheid
Professioneel-kritische instelling
SBR
Subsidies
Arbeidsmarkt
Beroep met toekomst
Derivaten
Financiering
Fraude en witwassen
Integrated reporting
Lerend vermogen
Onderzoek en wetenschap
Pensioen
Publiek belang
Semi-publieke sector
Van de Helpdesk