Stappenplan

Wat te doen bij een datalek

Voor accountants, boekhouders en ondernemers

Wolters Kluwer

Voor dienstverleners die met gevoelige data van klanten werken, is het voorkomen van schade door datalekken heel belangrijk. Een datalek kan grote schade veroorzaken aan het imago en de continuïteit van de eigen organisatie, en in sommige gevallen ook aan de persoonlijke levenssfeer van de betrokkenen. Toch kun je datalekken zelf bijna niet voorkomen. Natuurlijk doe je er als bedrijf alles aan om te voldoen aan de AVG en het lekken van privacygevoelige gegevens te voorkomen. Maar wat doe je als er toch data lekt? Dan is het belangrijk adequaat te handelen!

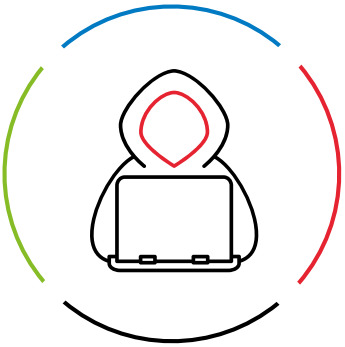
Hierbij een stappenplan.

1 Stel vast of het gaat om een datalek

Allereerst is het belangrijk om vast te stellen of er daadwerkelijk een datalek heeft plaatsgevonden. Een datalek is een inbreuk op de beveiliging die leidt tot vernietiging, verlies, wijziging of ongeoorloofde toegang tot persoonsgegevens. Het is dus alleen een datalek als er ongeluk of onrechtmatig persoonsgegevens:

- gestolen zijn door hacking, malware of phishing,
- vernietigd zijn (bijvoorbeeld door een brand),
- naar een verkeerde ontvanger zijn gestuurd (per e-mail of post),
- worden ingezien en/of bewerkt door niet-bevoegd personeel,
- verloren zijn gegaan (bijvoorbeeld een dossier dat in de trein is blijven liggen, telefoons, tablets en USB-sticks die zijn kwijtgeraakt),
- op een onrechtmatige manier zijn verwerkt. Bijvoorbeeld wanneer gevoelige data is opgeslagen zonder medeweten of toestemming van de betrokkene.
- langer dan de afgesproken periode zijn bewaard

Bekijk de meest voorkomende voorbeelden van een datalek.



2 Verzamel informatie

Het is van groot belang om zoveel mogelijk informatie in te winnen over het datalek:

- Welke persoonsgegevens zijn gelekt?
- Van wie?
- Wie kan toegang hebben gekregen tot de gegevens?
- Welke acties zijn al genomen?

Het is niet alleen belangrijk om te achterhalen hoeveel en welke gegevens precies gelekt zijn, maar vooral ook wat daar precies aan voorafging en hoe het lek heeft kunnen plaatsvinden.

Tip!

Bewaar alle correspondentie hierover, zoals e-mails en gespreksverslagen. Dit is heel belangrijk als toch de Autoriteit Persoonsgegevens op de stoep staat. Op deze manier kun je aantonen wat je als bedrijf hebt gedaan in het geval van een datalek

3 Stap 3. Stop een ‘actief’ datalek

Het kan zijn dat een datalek nog ‘actief’ is. Bijvoorbeeld wanneer een hacker of onbevoegde medewerker nog toegang tot de data heeft en nog altijd nieuwe gegevens kan buitmaken. Hackers blijven soms weken, maanden of zelfs jaren onopgemerkt in het netwerk en kunnen gedurende die tijd ongestoord data stelen. Maar ook medewerkers kunnen ongeoorloofd toegang hebben tot gegevens en zo een permanent datalek veroorzaken. In alle gevallen is het zaak zo snel mogelijk te handelen. Bijvoorbeeld door het blokkeren van accounts, het verplaatsen van de data naar een veilige locatie of het isoleren van een indringer van buitenaf.

9 onderzoeksvragen bij een datalek

1. Wat is de datum van het datalek?
2. Wat is de deadline wel/niet melden bij AP?
3. Wat is de datum van de ontdekking?
4. Wanneer is het onderzoek afgerond?
5. Wat is er gebeurd? Samenvatting van gebeurtenissen
6. Welke persoonsgegevens zijn gelekt?
7. Is de AP ingelicht ja/nee?
8. Indien risico voor betrokkenen gegevens: gemeld ja/nee?
9. Welke maatregelen zijn genomen om nog een keer te voorkomen?

4 Het datalek melden bij de Autoriteit Persoonsgegevens

Niet ieder datalek hoeft automatisch gemeld te worden. Je bent alleen verplicht melding te maken als het datalek mogelijkerwijs ‘ernstige gevolgen’ kan hebben voor de betrokkenen:

- zijn de gelekte gegevens gevoelig? (gezondheidsgegevens, BSN, handtekening, prestatiegegevens)
- zijn de personen kwetsbaar (zieken, kinderen, mensen die op de vlucht zijn voor bedreiging),
- wie heeft toegang verkregen, hoe heeft die gereageerd?

Als dit het geval is, meld het datalek dan binnen 72 uur via het meldloket van de Autoriteit Persoonsgegevens (AP).

Let op!

Het onterecht niet melden van een datalek brengt een forse boete met zich mee met een maximum van 825.000 euro of 10% van de omzet. Je kunt een melding altijd weer intrekken, mocht de schade of de gevolgen achteraf minder niet ernstig blijken. Neem dus het zekere voor het onzekere.

Bekijk het volledig AP-actieplan: ‘kom in actie bij een datalek’.

5 Betrokkenen informeren

Wanneer een datalek schadelijk is voor de persoonlijke levenssfeer van de betrokken personen, dan ben je verplicht hen te informeren. Dit is het geval wanneer:

- fysieke, materiële of financiële schade niet uit te sluiten is,
- medische gegevens verloren zijn, dan wel inloggegevens voor internetbankieren of een kopie van een paspoort op straat liggen,
- kans is op stigmatisering of reputatieschade,
- gegevens over iemands gedrag misbruikt kunnen worden, zoals gegevens over schulden, strafbare feiten of specifieke voorkeuren,
- Andere ernstige gevolgen kunnen zijn, bijvoorbeeld de locatie van een geheime verblijfplaats openbaar gemaakt wordt.

6 Schade beperken

Tips om verdere schade te voorkomen:

- Als van afstand gewist kan worden, doe dat zo snel mogelijk.
- Stuur een e-mail naar de verkeerde ontvanger en vraag om te wissen en dat te bevestigen.
- Is er een hack of malware, schakel – als het intern niet lukt – een specialist in om dit te helpen stoppen en een volgende aanval te voorkomen.

Tip!

Het kan zijn dat het niet altijd duidelijk is of betrokkenen ingelicht moeten worden. Schakel bij twijfel altijd een expert in.

Het melden van een lek aan de betrokkenen kan negatieve impact hebben op het imago van je organisatie. Openheid en eerlijkheid is echter heel belangrijk om (verdere) schade te voorkomen. Zorg dus voor een open bedrijfscultuur in je bedrijf. Zodat zaken niet onder de pet blijven en mensen durven te melden.'

Richard Ridderhof,
Compliance officer Twinfield

7 Maatregelen om een lek in de toekomst te voorkomen

1 Creëer bewustwording
Leg aan iedereen in het bedrijf uit wat de risico's zijn. Naast de boetes staat ook reputatie op het spel, en die is belangrijker! Herhaal deze boodschap en zorg voor meerdere momenten van bewustwording in het kader van datalekken.

2 Neem angst weg
Zorg ervoor dat werknemers die de oorzaak zijn, niet weg willen kruipen onder een bureau. Zodat ze bij een volgende keer wel onmiddellijk in actie komen.

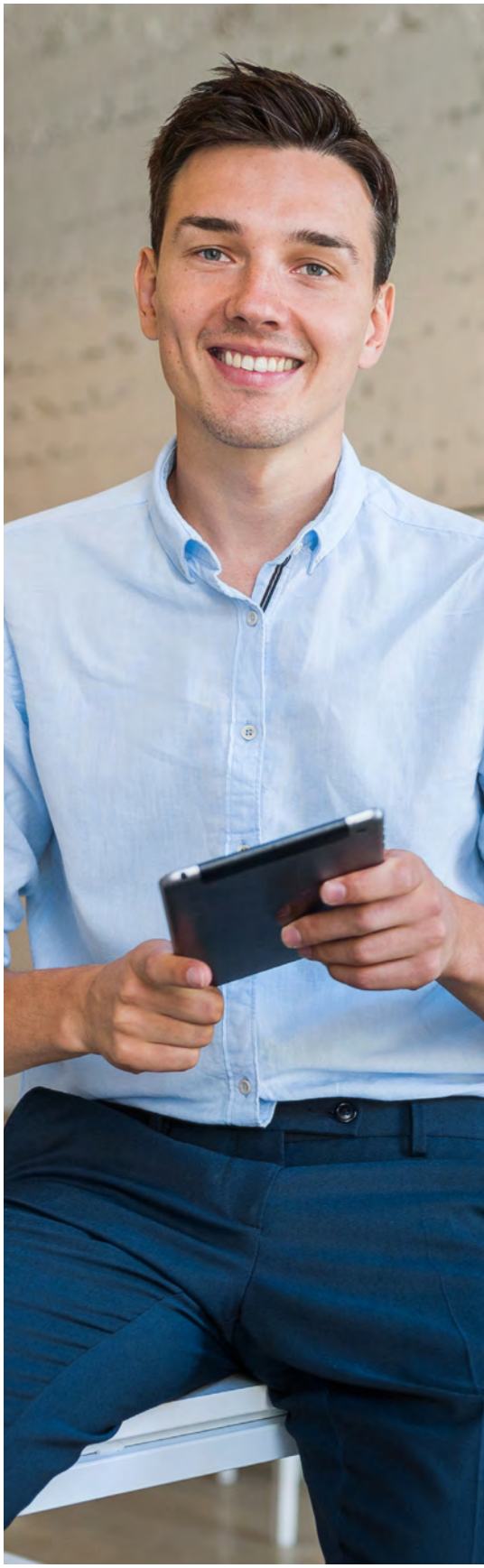
3 Hygiëneregels op orde
Het privacybeleid en de basis hygiëneregels moeten bij iedereen duidelijk zijn. Bijvoorbeeld nooit privacygevoelige gegevens op een memorystick, sluit een computer af wanneer je niet meer achter een bureau zit, laat je laptop niet in auto achter. Dit zijn kleine basistips die de kans op datalekken verkleinen.

4 Zorg voor een privacybeleid
Vaak ontstaan datalekken door een gebrek aan solide privacy-beleid, waardoor medewerkers bewust of per ongeluk zorgen voor een datalek. In zo'n beleid staat hoe de organisatie persoons-gegevens verwerkt, met welke doeleinden, en wie waartoe bevoegd en verantwoordelijk is. Vervolgens maak je afspraken met zowel je eigen medewerkers als de direct betrokkenen hierover.

5 Leg een datalekprotocol vast
Leg vast in een protocol wie er gebeld moet worden als het misgaat. En wat er vervolgensallemaal moet worden gedaan om schade te beperken. Dat geldt ook voor kleine bedrijven! Weet ook wie je moet bellen bij welke externe leveranciers in het geval bij een datalek. Houd iedereen scherp en trek lessen uit wat er is gebeurd. Processen zijn niet in beton gegoten! Ze moeten periodiek geupdate worden.

6 Investeer in technische security middelen
Was het lek te wijten aan onvoldoende technische security-maatregelen? Investeer dan in betere security-middelen.

7 Ga veilig om met gegevens
Als je veilig om wil gaan met gegevens, is het van belang dat je goed nadenkt wat je echt wilt weten. Vraag geen geboortedatum als dat niet nodig is. Houd je aan je doel waarom je gegevens opslaat. De Autoriteit Persoonsgegevens deelt echt boetes uit aan organisaties die gegevens gebruiken voor een ander doel dan opgeslagen.



Dit stappenplan wordt je aangeboden door Twinfield

Twinfield Boekhouden is een professioneel en compleet online boekhoud-programma, waarmee je slim en gemakkelijk online samenwerkt met je accountant. Twinfield Boekhouden koppelt met bijna alle webwinkelsoftware. Zo worden je verkopen eenvoudig geregistreerd en heb je actueel inzicht in de resultaten. Je gegevens zijn zeer veilig en je werkt volledig in de cloud. Twinfield Boekhouden werkt ook goed bij grote aantallen transacties en helpt je bij foutloze btw-aangiftes.

Over Wolters Kluwer

Wolters Kluwer is een van de grootste aanbieders van informatie, software, tools en diensten voor juridische en fiscale professionals. Wereldwijd werken honderd-duizenden van hen elke dag met onze software. Voor hun dagelijks werk vertrouwen zij op onze jarenlange expertise en op onze producten. De divisie Tax & Accounting levert professionele software, waaronder Twinfield Boekhouden, Twinfield Samen-werken, Alure Online, Basecone en Avanzer Aangifte.

Contact

Twinfield | De Beek 9-15
3871 MS | Hoevelaken | The Netherlands
www.twinfield.nl | +31 (033) 467 70 10

Wolters Kluwer