RendementOnline

Zo gaat u om met datalekken in 5 stappen

Hoe u een datalek kunt voorkomen en wat te doen als het toch gebeurt

CHECKLIST
Publicatiedatum:
13 juli 2023

Een datalek zit in een klein hoekje. Van een verloren usb-stick of een vergeten laptop, tot verkeerd bezorgde post of een hack van uw systemen.
Een datalek kan schadelijk zijn voor uw werknemers en uw klanten, wanneer hun persoonsgegevens op straat komen te liggen, én het kan schadelijk zijn voor het imago van uw organisatie. Ook niet onbelangrijk: als u niet kunt aantonen dat u er alles aan heeft gedaan om het datalek te voorkomen, kan de Autoriteit Persoonsgegevens een boete opleggen.
In deze toolbox leest u wat u moet weten over datalekken, hoe u ze moet voorkomen en vooral, hoe te handelen als er een datalek plaatsvindt.

Deze toolbox bestaat uit de volgende stappen:

Voorkom datalekken en weet wat te doen als ze toch gebeuren

Een datalek kan uw organisatie zomaar overkomen, maar dat betekent niet dat u er niet alles aan moet doen om datalekken te voorkomen. Niet alleen is een datalek op zijn minst erg vervelend voor de betrokken werknemers of externe contacten, ook kan de eventuele boete hoog zijn. Hierover leest u meer in het eerste gedeelte van deze toolbox. Mocht er onverhoopt toch een datalek plaatsvinden in uw organisatie, volg dan de juiste stappen. Licht alle betrokkenen in en meld het datalek bij de Autoriteit Persoonsgegevens (AP). Verderop in deze toolbox staat wat u precies moet doen, en vindt u handige tools die u helpen met die stappen.

Stap 1 Download de interactieve checklist

☐  CHECKLIST Zo gaat u om met datalekken in 5 stappen

De eerste checklist heeft u nu voor u. Hierin staan alle onderdelen van deze toolbox benoemd. U kunt de status van de te nemen stappen in deze checklist bijhouden en afvinken welke onderdelen u heeft afgerond. Dit vinkje kunt u dus vast zetten.

Opmerkingen

Stap 2 Wat u moet weten over datalekken

☐  NIEUWS Datalek persoonsgegevens slechts een kwestie van tijd

Van elk individu zijn er al een keer persoonlijke gegevens gelekt of gaat dit nog gebeuren, stelt de AP. Het is daarom van belang om het beschermen van de eigen persoonsgegevens goed op te pakken. Dit meldt de AP naar aanleiding van de recent verschenen jaarlijkse datalekkenrapportage. In dit nieuwsartikel vindt u een aantal tips voor de bescherming van persoonsgegevens.

Opmerkingen

NIEUWS [Meer kans op datalekken bij grote organisaties]

Hoe groter de organisatie, hoe groter de kans op datalekken, aldus de Cybersecuritymonitor 2020 van het CBS. In 2019 kreeg 25% van organisaties met 250 of meer werknemers te maken met datalekken, waarbij een intern incident de oorzaak was. Daarnaast had 8% van deze organisaties te maken met datalekken door een aanval van buitenaf. Meer cijfers over datalekken leest u in dit nieuwsartikel.

Opmerkingen

NIEUWS [Merendeel datalekken door verkeerd bezorgde post]

Incidenten met het versturen van brieven en postpakketten zijn de belangrijkste oorzaak van datalekken. Dat blijkt uit de 'Jaarrapportage meldplicht datalekken 2021' van de AP. Lees in dit nieuwsartikel wat de veelvoorkomende oorzaken van datalekken zijn.

Opmerkingen

Stap 3 Datalekken en de Algemene verordening gegevensbescherming (AVG)

ARTIKEL [Hoe ziet de meldplicht datalekken eruit onder de AVG?]

De meldplicht datalekken is een belangrijk onderdeel van privacyrichtlijn AVG, en de boetes voor het lekken van data zijn behoorlijk hoog. Lees dit verdiepingsartikel, zodat u weet hoe de meldplicht datalekken eruitziet onder de AVG en u niet voor verrassingen komt te staan.

Opmerkingen

TOOLBOX [Voldoe aan de AVG in 9 stappen]

De strenge privacyregels van de AVG hebben betrekking op alle gevallen waarbij persoonsgegevens worden opgeslagen en verwerkt. Inmiddels mag van organisaties wel verwacht worden dat de AVG geïmplementeerd is in de operationele processen. Toch blijken er nog steeds onduidelijkheden te zijn, en is een onbedoelde overtreding van de AVG snel begaan. Deze toolbox bevat de belangrijkste tools en uitleg om te zorgen dat uw organisatie echt voldoet aan de AVG.

Opmerkingen

Stap 4 Voorkom datalekken

ARTIKEL [Het veilig delen van persoonsgegevens]

De basis voor privacybescherming en informatiebeveiliging is het analyseren en beheersen van risico's. Zonder risico's zouden er geen maatregelen voor bescherming nodig zijn. Helaas is het maar al te waar dat iets kleins tot een groot risico kan leiden: zelfs een e-mail naar een verkeerde persoon verzenden kan al een datalek inhouden. Lees het in dit verdiepingsartikel hoe u uw e-mail beveiligt.

Opmerkingen

NIEUWS [Digitaliseren uitbesteden kan datalek betekenen]

Pas op met het uitbesteden van projecten waarbij persoonsgegevens een rol spelen. Twee ziekenhuizen zijn namelijk tot de ontdekking gekomen dat het bedrijf dat zij hadden ingehuurd om patiëntendossiers te digitaliseren, deze door gedetineerden 'scanklaar' liet maken. In dit nieuwsartikel leest u waarom uw organisatie bij het uitbesteden verantwoordelijk blijft voor de beveiliging van persoonsgegevens, en welke rol de ondernemingsraad hierbij kan spelen.

Opmerkingen

NIEUWS

Metadata in documenten kunnen zorgen voor een datalek

Ook documenten kunnen namen bevatten van medewerkers. Op het moment dat die documenten met de buitenwereld gedeeld worden, kan er sprake zijn van een datalek. Niet iets waar u meteen aan denkt, zoals ook de AP zelf ondervond. Hoe dit kan, en hoe u die metadata kunt anonimiseren, leest u in dit nieuwsartikel.

Opmerkingen

V & A

Hoe voorkomen we datalekken bij thuiswerken?

Het is belangrijk dat u uw werknemers opdraagt om, als dat mogelijk is, uitsluitend in een beveiligde thuiswerkomgeving te werken. Dus laat werknemers thuis inloggen op de server van uw organisatie. Als het goed is krijgen werknemers dan hetzelfde scherm te zien als op kantoor. Het handigst is het als de werknemers apparatuur gebruiken van kantoor, zoals laptops en tablets. Meer tips vindt u in deze Vraag & Antwoord.

Opmerkingen

V & A

Hoe kunnen wij de informatie op oude harde schijven wissen?

Opslagmedia moeten nooit zomaar worden doorverkocht. Zeker voor organisaties is het van groot belang om de data grondig te wissen, zodat zij voorkomen dat er bedrijfsgeheimen op straat komen te liggen. Dat gaat lang niet altijd goed. Vaak zijn er nog gevoelige gegevens te vinden op opslagmedia die online te koop staan. In deze Vraag & Antwoord leest u hoe u deze gegevens grondig kunt wissen.

Opmerkingen

TOOLBOX [Zo verbetert u de cybersecurity van uw organisatie]

Berichten over hacks, ransomware, phishing en andere cybercrime zijn letterlijk dagelijks nieuws. Het lijkt erop dat het niet de vraag is of uw organisatie getroffen wordt door een cyberaanval, maar eerder wanneer en hoe. En vooral: hoe groot is de schade en hoe snel is deze hersteld. In deze toolbox leest u niet alleen hoe uw organisatie zich zo goed mogelijk kan beschermen tegen digitale aanvallen, maar ook hoe uw werknemers daaraan kunnen bijdragen, en hoe u zo goed en snel mogelijk de schade herstelt.

Opmerkingen

Stap 5 Als er toch een datalek is

V & A [Moet ik een datalek altijd melden?]

Uw organisatie is verplicht om de personen in te lichten van wie de persoonsgegevens bij het datalek bloot zijn komen te liggen als het lek een hoog risico vormt voor rechten en vrijheden. Er zijn wel uitzonderingen op de meldingsplicht, maar daarvoor gelden wel voorwaarden. Lees in deze Vraag & Antwoord wanneer uw organisatie een datalek niet aan de gedupeerden hoeft te melden.

Opmerkingen

CHECKLIST [Voldoen aan de meldplicht datalekken]

Datalekken kunnen ontstaan doordat er bijvoorbeeld een laptop met belangrijke persoonsgegevens wordt gestolen. Een melding hoeft niet in alle gevallen te worden gemaakt, maar in ieder geval wel in gevallen waarbij een aanzienlijke kans op ernstige nadelige gevolgen is, of als deze gevolgen heeft voor de bescherming van persoonsgegevens. Aan de hand van deze checklist kunt u bepalen of u melding moet maken van een datalek en, als dat het geval is, welke stappen u precies moet nemen.

Opmerkingen

REGLEMENT

Procedure datalekken en beveiligingslekken

Niemand wil het, maar het gaat soms toch fout: er ontstaat een data- of beveiligingslek. Met een vooraf vastgelegde procedure bent u beter voorbereid op de hectische situatie die hierdoor kan ontstaan. Met een data- en beveiligingslekprocedure zorgt u ervoor dat u het lek snel en efficiënt onderzoekt, op de juiste wijze documenteert en meldt bij de juiste personen en instanties. Ook verkleint u de kans op herhaling. Deze tool helpt u bij het opstellen van een dergelijke procedure.

Opmerkingen

MAATWERKBRIEF

Datalek melden aan betrokkenen

Door de meldplicht datalekken bent u verplicht om bij een datalek de betrokkenen hiervan op de hoogte te stellen. Dit is alleen het geval als het datalek invloed heeft op de rechten en vrijheden van de betrokkenen. De meldplicht datalekken is onderdeel van de AVG. Met deze maatwerkbrief stelt u betrokkenen op de hoogte. U kunt kiezen uit een je-versie en een u-versie.

Opmerkingen

FORMULIER

Incidentregistratie bij datalekken

De AVG verplicht organisaties om documentatie bij te houden van alle datalekken die hebben plaatsgevonden. In dit formulier kunt u eenvoudig van elk potentieel datalek alle verplichte informatie registreren. Het ingevulde tabblad Registratiebeheer kan door de AP worden opgevraagd. U bent in dat geval verplicht inzage te verlenen in dit document.

Opmerkingen

NIEUWS Datalek niet tijdig melden is dubbele fout

Het kan iedereen gebeuren, al is het natuurlijk niet fraai: data lekken. Maar áls het gebeurt, is het belangrijk om het datalek binnen 72 uur te melden bij de AP. Als een organisatie verzuimt dat te doen, is dat fout op fout. Het kwam een afdeling van een politieke partij op een forse boete te staan. Lees hoe dat zit in dit nieuwsartikel.

Opmerkingen

Stap 6 De rol van de OR bij datalekken

NIEUWS AP maakt melding datalek eenvoudiger

Er zijn genoeg redenen voor de ondernemingsraad (OR) om het onderwerp 'datalekken' bij de bestuurder op de agenda te zetten. Het is belangrijk dat de organisatie een protocol voor datalekken opstelt, en de OR betrekt bij het opstellen en actualiseren van dit protocol. Vervolgens moet hij het protocol ter instemming voorleggen aan de OR. De OR heeft namelijk instemmingsrecht bij regelingen rond de bescherming van persoonsgegevens. In dit nieuwsartikel leest u meer over de rol van de OR bij het privacybeleid.

Opmerkingen

Toch nog vragen?
Als u na het bestuderen van deze toolbox nog vragen heeft over datalekken, kunt u die voorleggen aan de adviseurs van de adviesdesk. Stel als abonnee gratis uw vraag via rendement.nl/adviesdesk en ontvang binnen vijf werkdagen een antwoord.