Datalek: better call the IRT!

Sinds de invoering van de Algemene Verordening Gegevensbescherming (AVG) zal menig organisatie klamme handen krijgen bij de gedachte aan een datalek. Uit het toenemend aantal nieuwsberichten over datalekken en opgelegde boetes blijkt dat een datalek geen 'ver-van-je-bed-show' meer is: een datalek kan iedere organisatie overkomen. Maar wat is een datalek nu precies en wat moet men ermee?

Een voorbeeld: een werknemer van een uitzendbureau komt op donderdagochtend met de trein naar het werk, maar vergeet een map met daarin 50 CV's van uitzendkrachten mee te nemen. Op kantoor aangekomen ontdekt de werknemer de fout en neemt contact op met de NS. Helaas, aan het einde van de dag is de map nog steeds niet terecht. Op vrijdagochtend meldt de werknemer de verloren map bij zijn leidinggevende, die op zijn beurt op vrijdagmiddag het incident meldt bij de kantoormanager. De kantoormanager is echter al naar huis en pakt de zaak dus op maandagochtend op…

…klinkt het voorgaande scenario realistisch? Leest u dan verder. Denkt u dat zoiets niet in het echt gebeurt? Hierbij een waargebeurd verhaal:

In september dit jaar werd een medewerker van het Haga Ziekenhuis ontslagen, omdat de medewerker een A4tje met medische gegevens van patiënten had gebruikt als boodschappenlijstje. Vervolgens had de medewerker dit document in het boodschappenmandje laten liggen, waar het door iemand anders werd gevonden. Een datalek dus. Pijnlijk, voor de patiënten en de medewerker, en zeker ook voor het ziekenhuis, dat twee maanden ervoor nog een boete van € 460.000 had gekregen voor een ander datalek.

Uit bovenstaande voorbeelden blijkt al dat datalekken zich op allerlei manieren voordoen. Andere voorbeelden van veel voorkomende (potentiële) datalekken zijn: diefstal van een smartphone of laptop, besmetting van IT-systemen van de organisatie met ransomware[1] of het versturen van een mail met personeelsgegevens aan een verkeerde ontvanger. Er is dus lang niet altijd kwade opzet bij een datalek, vaak ontstaan datalekken simpelweg door menselijke fouten.

En nu praktisch: wat moet er gebeuren bij een datalek?
Zoals met veel zaken is voorkomen beter dan genezen. Het is niet realistisch om te denken dat alle datalekken kunnen worden voorkomen, maar door werknemers regelmatig te trainen en bewust te maken van gevaren bij het werken met persoonsgegevens wordt de kans wel verkleind. Als dan toch een datalek ontstaat is snel handelen geboden. Datalekken moeten binnen 72 uur worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) vanaf het moment dat het datalek is ontdekt.

Deze periode van drie dagen lijkt misschien lang, maar de ervaring leert dat dit voor het melden van een datalek juist erg kort is. In het eerste voorbeeld zou het bedrijf bijvoorbeeld al te laat zijn met de melding. Naast de juiste personen in de onderneming informeren, is onderzoek nodig en moeten er verschillende (risico)schattingen worden gedaan en besluiten worden genomen. Deze besluiten zijn niet zonder belang: zowel in gevallen waarbij een datalek niet aan de autoriteit was gemeld (Uber in 2018) en waar wel een melding was gedaan (Marriott Hotels in 2019) zijn boetes opgelegd door de toezichthouder.

Door het inschakelen van een Incident Response Team (IRT) worden bedrijven in staat gesteld om adequaat te handelen bij een datalek. Een IRT bestaat uit verschillende disciplines, waaronder vaak forensische IT-experts, juristen en eventueel communicatie experts en wordt onder andere aangeboden via cyberverzekeringen. Wij maken regelmatig deel uit van een IRT en wij ervaren dat de directe en doelgerichte hulp van zo'n team de negatieve consequenties van een datalek effectief kan bestrijden, onder meer door tijdige melding en het contact met de Autoriteit Persoonsgegevens te onderhouden. Dit kan het verschil betekenen tussen een afloop met een sisser en een boete of imagoschade.

Dus is er een datalek? Keep calm and call the Incident Response Team!

Door Rosalie Brand
Kennedy Van der Laan
Lid van diverse incident response teams

1) Ransomware (of gijzelsoftware) is een chantagemethode waarbij digitale bestanden worden versleuteld en er losgeld wordt gevraagd om deze bestanden te ontsleutelen.