Factsheet

Datalek Preventie in de zorg

Er staan voor zorginstellingen in 2016 twee belangrijke wetswijzigingen op het gebied van Data Privacy op stapel:

1. Meldplicht datalekken

Met de meldplicht datalekken wil de regering de gevolgen van een datalek voor de betrokkenen zoveel mogelijk beperken en hiermee een bijdrage leveren aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens.

Deze meldplicht geldt voor alle verantwoordelijken voor de verwerking van persoonsgegevens, zowel in de private als publieke sector. Als er geen melding wordt gemaakt van een datalek kan dit bestraft worden met een bestuurlijke boete van het CBP die kan oplopen tot €810.000,- of, als dat niet passend is, 10% van de jaaromzet van de rechtspersoon,

2. Aanpassing van de Europese privacy wetgeving

In de loop van 2016 zal naar verwachting de nieuwe privacy verordening worden goedgekeurd. Deze wetgeving zal de Europese Privacy richtlijn van 1995 vervangen en de maatstaf vormen voor nationale wetgeving op Data Privacy.

Deze nieuwe Europese wetgeving bevat strengere privacy regels dan de huidige Wet Bescherming Persoonsgegevens (WBP). Bij het niet voldoen aan deze regelgeving kan een boete van maximaal €100 miljoen opgelegd worden of, als dat niet passend is, 5% van de wereldwijde jaaromzet van de rechtspersoon.

Gevolgen voor zorginstellingen

De kerntaken van vooral een ziekenhuis zijn zorg en onderzoek. Patiëntgegevens (privacy gevoelige gegevens) zijn voor het uitvoeren van zorg en onderzoek van groot belang en daarvoor worden patiëntgegevens verzameld, opgeslagen en bewerkt. Vanwege deze activiteiten is het daarom van belang dat voldoende aandacht besteed wordt aan het adresseren van deze data privacy, zodat sancties en reputatieschade zoveel mogelijk worden voorkomen.

Het vertrouwen op het geïmplementeerde informatiebeveiligingsbeleid is niet voldoende, de bescherming van data moet bij de eindgebruiker worden verankerd. Deze eindgebruiker is namelijk (onbedoeld) de grootste veroorzaker van datalekken.

Bovenstaande overwegende maakt dat een ziekenhuis in onze visie een zeer groot risico loopt op privacy incidenten. De sanctionering bij het niet melden of het onjuist melden is van dien aard dat een ziekenhuis een behoorlijk financieel risico loopt, los van de gevolgschade voor het ziekenhuis en de patiënt.

Voorkomen is beter dan...

Om datalekken te voorkomen is het voor zorgorganisaties van belang om antwoord te krijgen op vragen als:

- Wat is gevoelige informatie/data (bijv. patiëntgegevens)?
- Waar staat deze informatie (systemen, machines)?
- Waar gaat deze vertrouwelijke informatie naar toe?
- Waar is de ontvanger van die informatie klaarblijkelijk toe geautoriseerd (openen, lezen, wijzigen, emaillen, kopiëren, etc.)?

Ondanks het naleven van richtlijnen vanuit een vigerend beveiligingsbeleid is een menselijke interventie vaak de oorzaak van een datalek. Een Data Lek Preventie (DLP) oplossing voorkomt dat deze menselijke interventies kunnen optreden.

Datalek Preventie in de zorg

Bottum-up Aanpak

Er zijn verschillende manieren om data te beschermen en bovenstaande risico's te verkleinen:

- Een *"top-down"* procesmatige aanpak, startend vanuit Privacy Impact Analyses en vanuit daar verbeteringen doorvoeren;
- Een aanpak die zich *"bottom-up"* richt op inzicht welke informatie door wie wordt bewerkt en verstuurd.

Atos heeft goede ervaringen opgedaan met de "bottom-up" aanpak, mede door gebruik te maken van hiertoe ontwikkelde Datalek Preventie tooling van het bedrijf Digital Guardian. Volgens onderzoeksbureau Gartner één van de toonaangevende spelers op dit gebied[1].

De bottom-up aanpak geeft antwoord op de bovenstaande vragen, door bij de huidige situatie van de zorginstelling te beginnen en daar de risico's met betrekking tot privacy gevoelige informatie inzichtelijk te maken.

1 *Gartner Magic Quadrant for Enterprise Data Loss Prevention, Published: 28 January 2016*

Voorstel

Wij willen u graag laten zien wat de datalek preventie oplossing voor uw zorgorganisatie kan betekenen. Ons voorstel is dat wij een "proof-of-concept" (PoC) uitvoeren voor een beperkte set van classificatie van gegevens. Deze proof-of-concept bestaat uit drie fasen (zie figuur 1).

- Bewustwordingsworkshop;
- Haalbaarheidsonderzoek;
- Workshop met daarin een overzicht van de resultaten uit het haalbaarheidsonderzoek.

Implementatie vervolgtraject

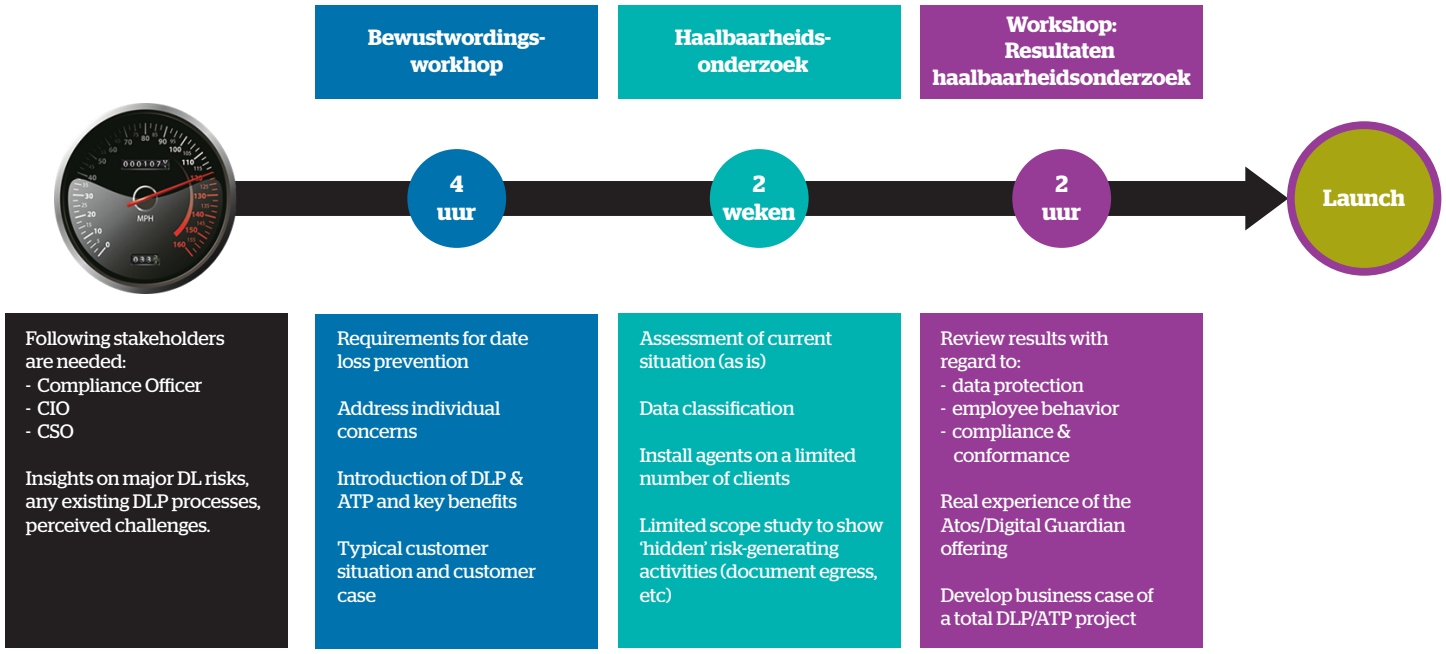
U kunt ervoor kiezen op verschillende manieren om tot een implementatie te komen: per vakgroep/ cluster/divisie, klinisch/poliklinisch, per rol etc.

Voor de installatie kan gekozen worden uit een CAPEX (uw locatie) of OPEX (Atos Managed Services) model. De Managed Service variant wordt beheerd vanuit een Nederlands Datacentrum.

Aanbod

Deze Proof-of-Concept, conform de bovengenoemde fasering bieden wij aan voor een bedrag van € 10.000,- exclusief BTW.

Figuur 1: Fasering en aanpak Proof-of-Concept



Voor meer informatie:
Herman van den Tempel
Director Healthcare Benelux & the Nordic Countries
+31 (0)6-54 37 44 17
Herman.vandentempel@atos.net