5 datasecurity-KPI's die uw onderneming zeker moet meten

U en uw medewerkers doen ongetwijfeld de nodige inspanningen om GDPR-compliant te zijn. Maar worden de juiste en efficiëntste inspanningen geleverd? Hou aan de hand van deze 5 KPI's uw GDPR-status bij. Ze geven u een klare kijk of uw onderneming goed bezig is op het gebied van dataprivacy.

1. Percentage privacyaanvragen die binnen de wettelijke tijd zijn afgehandeld

Elke persoon kan op elk moment bij uw onderneming informeren welke gegevens u over hen bezit. Uw onderneming moet daarbij binnen de maand gepast reageren door de persoon in kwestie een kopie van de persoonsgegevens, plus informatie over hoe de gegevens zijn gebruikt, te bezorgen. Volgt u deze procedure niet, dan kunnen sancties worden opgelegd. Of uw medewerkers correct en op tijd handelen, kan u meten aan de hand van deze formule:

Aantal privacyaanvragen dat binnen de wettelijke tijd is afgehandeld / totaal aantal servicevragen.

Idealiter staat dit percentage gelijk aan 100.

2. Positieve gegevensbeschermingseffectbeoordeling

GDPR verplicht om een **interne documentatie** bij te houden van de verwerkingsactiviteiten en de veiligheidsmaatregelen in uw bedrijf.

Deze gegevensbeschermingseffectbeoordeling (GEB) moet minstens de volgende elementen bevatten:

- Een gedetailleerde beschrijving van de verwerkingen en verwerkingsdoeleinden
- Een beoordeling van de evenredigheid van de verwerkingen in functie van de doeleinden
- Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen
- De beoogde maatregelen om de risico's aan te pakken

Een GEB is enkel **verplicht voor nieuwe processen**, maar de Privacycomissie raadt ook aan een risicoanalyse uit te voeren op de lopende processen met een hoog risico. Uw DPO is verantwoordelijk voor de uitvoering van de GEB. Hij zal dan naargelang de resultaten **aansluitende adviezen** geven, die u helpen KPI's op te stellen of bestaande KPI's aan te passen.

5 datasecurity-KPI's die uw onderneming zeker moet meten

3. Tijd tot detectie en oplossing

Indien een bepaald incident (datalek, misbruik ...) een risico inhoudt voor de betrokkenen moeten zij en de toezichthoudende autoriteit **binnen de 72 uur op de hoogte gesteld worden van de inbreuk**.

Voor de reputatie van uw bedrijf en voor de betrokkenen is het dus van cruciaal belang om na een incident zo snel mogelijk te reageren en een oplossing te vinden. Er zijn eenvoudige manieren om het **tijdsbestek te meten en te monitoren**. Probeer een tool als *Toggl*, zodat uw team gezamenlijk alle minuten en uren kan bijhouden.

4. Aantal kleine en grote veiligheidsincidenten

Het ligt voor de hand om grote datalekken of inbreuken tegen de GDPR te meten en te monitoren. Daarnaast moet u ook zeker oog hebben voor kleinere incidenten of *near misses*, want deze zijn vaak een kwaadaardige test die kan uitgroeien tot een volledige aanval. Een voorbeeld van een kleiner beveiligingsincident kan een **e-mailphishing**-zwendel zijn of een **ongebruikelijke activiteit op uw server**.

Het is zeker niet zo dat één klein incident veel invloed zal hebben op uw bedrijf, afgezien van frustratie en het feit dat het een ontnuchterende wake-upcall is. Maar honderden kleine incidenten of bijna-incidenten vragen **voortdurende inspanningen en kosten** die oplopen en lijken op het prijskaartje dat gepaard gaat met een grotere hack. Behoud dus het overzicht van het aantal kleine en grote veiligheidsincidenten en pas waar nodig uw veiligheidsbeleid aan.

5. Kosten per incident

De kosten per hackincident gaan verder dan wat uw bedrijf uitgeeft om een aanval op te lossen. Het is verstandig om te kijken naar zowel de kosten per incident als het aantal individuele dossiers. U moet rekening houden met de kosten voor:

- het cyberonderzoek,
- extra personeel en overuren om het incident in te dijken,
- een PR-campagne om het publiek aan te spreken.

Het is mogelijk dat uw communicatie- en PR-reactie meer kost dan het herstellen van uw gegevens en het verwijderen van malware uit uw systemen. Ga daarom zeker even samenzitten met uw beveiligingsteam en kijk naar alle gevolgen rond de aanval en welke middelen nodig waren om de aanval op te lossen.

Bron: Europese Commissie

Het volledige overzicht bewaren over uw GDPR-beleid?

Ontdek de voordelen van GDPR Compliance Software →