Case 1: Cyber Security

Adviseer Team DSM om persoonlijke en concurrentiegevoelige data veilig te verzamelen, delen en gebruiken binnen de organisatie.

Achtergrond

Team DSM is een professionele wielerorganisatie die meedoet op het hoogste niveau; de UCI WorldTour. De organisatie heeft 3 teams: het elite heren team, het elite damesteam en het development team. Het hoofdkantoor van Team DSM bevindt zich in Deventer en de campus waar het development team verblijft en traint is in Sittard. De renners van het elite team trainen door het jaar heen individueel en zijn alleen bij elkaar tijdens trainingskampen, wedstrijden en andere teamevenementen. Daarnaast werkt Team DSM samen met meerdere partners die een rol spelen binnen de organisatie zoals bijvoorbeeld met KPMG op het gebied van data-analyse en digitale transformatie.

Om zo goed mogelijk te presteren in een wedstrijd, wordt er veel data verzameld over de wielrenners. Er worden medische testen gedaan, maar ook real-time data verzameld tijdens trainingen en officiële ritten. Tegelijkertijd is het supportteam rondom de wielrenners erg dynamisch. Voor belangrijke wedstrijden wordt er opgeschaald en verschillende partners hebben ook toegang nodig tot sommige elementen van de verzamelde data om hun werk te doen.

De case: beveiliging van data van Team DSM

Het is van belang dat alle data die verzameld wordt goed beveiligd is. Wanneer er medische data lekt is dit niet alleen heel vervelend voor de renners. Het kan, in combinatie met bijvoorbeeld real-time data, enorm concurrentiegevoelige data zijn.
We gaan uit van een ‘green field’ situatie: Team DSM heeft op dit moment nog niets op het gebied van cyber security ingericht.

De vraag aan jou: ontwikkel een stappenplan om de risico’s rondom dit data-vraagstuk te dichten.
Een aantal suggesties om je op weg te helpen:

- Hoe ga je om met alle medewerkers die toegang tot data hebben?
- Hoe richt je de technische beveiliging van de data die van fiets naar cloud naar laptop in de auto wordt gestuurd in?
- Hoe ga je om met het feit dat er binnen Team DSM een mogelijke infiltrant van een ander team aanwezig is?

Om dit stappenplan te maken is het handig om na te denken over de volgende aspecten:

- Wat is het dreigingslandschap van Team DSM?
- Wat zijn de risico’s die als eerste afgedekt moeten worden?
- Wat zijn de “kroonjuwelen” van Team DSM? (met andere woorden: wat zijn de belangrijkste zaken om te beveiligen?)

Zo stuur je je antwoord in

Om de inzendingen goed met elkaar te kunnen vergelijken vragen we je om maximaal 4 A4'tjes in te leveren. Hierin zien we graag de volgende elementen terug:

- De risico's voor Team DSM
- De acties die genomen moeten worden om de risico's te dichten
- De winst/voordelen die deze acties met zich meebrengen

Wees creatief en weet dat alle verbeteringen op het gebied van cyber security er al voor kunnen zorgen dat Team DSM optimaal kan presteren!

Stuur je inzending naar KPMGchallenge@kpmg.nl en wie weten nodigen we je uit voor een gesprek voor een baan bij KPMG.

Vermeld duidelijk welke case je antwoord op geeft, je voor- en achternaam.