VEILIG OMGAAN MET KLANTGEGEVENS IS EEN MUST **VOOR ELKE FITNESSONDERNEMER**

De toenemende digitalisering van onze samenleving brengt niet alleen nieuwe mogelijkheden, maar ook nieuwe uitdagingen mee. In de afgelopen tijd heb ik vaak geschreven over de voordelen die digitalisering meebrengt voor fitnessondernemers en hoe het vergaren van data ongekende mogelijkheden biedt voor de personalisering van fitness.

Klantgegevens die trainers en clubs binnenkrijgen via apps en wearables geven heel veel informatie – zo krijgen ze namelijk gedetailleerd inzicht in de levensstijl van klanten, en kunnen ze trainings- en voedingsprogramma's tot in de puntjes personaliseren. Zo krijgen moderne fitnessconsumenten waar ze naar verlangen: op maat gemaakte fitness- en gezondheidsdiensten die leiden to duurzaam succes met persoonlijke aandacht.

En dus wordt beveiliging van data en persoonsgegevens steeds belangrijker onderwerp voor de fitnessindustrie. Dus hoe worden datalekken veroorzaakt, wat zijn de gevolgen – en misschien wel het belangrijkste – hoe voorkom je ze als fitnessondernemer?

Een datalek zit in een klein hoekje

Bij een datalek denk je snel aan hackers die op een donkere zolderkamer persoonsgegevens stelen om ze door te verkopen aan andere kwaadwillenden. Die bestaan zeker ook, maar verreweg het grootste gedeelte van datalekken – zo'n 66% volgens de Autoriteit Persoonsgegevens – komt door menselijke fouten. Dat komt er eenvoudigweg op neer dat klantgegevens door een onbedoelde actie op straat komen te liggen. En dat is zeker niet altijd een gecompliceerd technisch verhaal, het kan zo eenvoudig zijn als een massamail uitsturen naar klanten waar iedereen in de CC staat in plaats van de BCC. Dat is vervelend bij het uitsturen van een algemene nieuwsbrief, maar als er per ongeluk meer persoonlijke informatie wordt gedeeld zoals slaap- en eetpatronen, gewicht, vetpercentage etc., zal het vertrouwen van klanten die deze gegevens delen vele malen erger worden geschaad.

De bekendste voorbeelden van datalekken in de fitnessindustrie komen precies door zulke menselijke fouten. Zo waren de online fitnesstrackers Strava en FitBit tot 2018 populair onder Amerikaanse militairen – tot Strava een wereldwijde heatmap publiceerde met de meest gelopen routes. Een leuk idee, behalve dat ze daarmee ook de ligging van verschillende basissen en patrouilleroutes in conflictgebieden bekendmaakten. Fitnesstrackers zijn nu grotendeels verboden voor gestationeerde militairen of op uitzending, ook in Nederland. In 2021 werden bovendien de gegevens van 61 miljoen wearable-dragers gelekt die waren aangesloten bij het platform GetHealth omdat een medewerker was vergeten de online database te beveiligen met een wachtwoord. Een menselijke fout zit dus in een klein hoekje. Nu zijn dit grootschalige voorbeelden, maar ook op kleinere schaal heeft dit zeker ook impact.

Voor ondernemers zijn de gevolgen van zo'n dergelijk datalek dan ook tweeledig. Ten eerste hebben we allemaal te maken met de privacywetgeving, AVG. De Autoriteit Persoonsgegevens beboet overtredingen van de privacywet – en dat kan hoog oplopen. Boetes gaan tot maximaal 20 miljoen euro of 4% van de jaaromzet.

Ten tweede is er langdurigere imagoschade voor je bedrijf, denk dan vooral aan minder waardering voor je merk door het geschade klantvertrouwen. Een boete kun je afbetalen en dan is het ook klaar, maar beschadigd vertrouwen in je merk kan maanden tot jaren duren voordat je het weer hebt opgebouwd. En dat loopt in de kosten: klanten die hun abonnement opzeggen, het opdrogen van leads, slechte reviews online – het is allemaal langdurige financiële schade die ondernemers oplopen na een datalek.

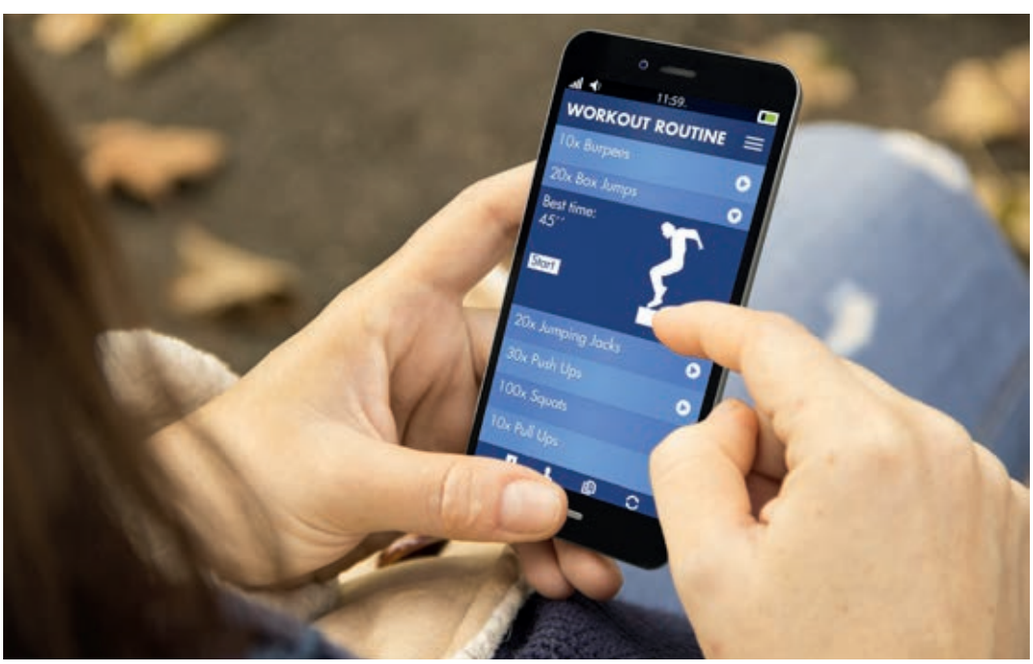
Veilig werken is een financieel gezonde keus

Nooit eerder deelden consumenten zo vrijelijk details over hun privéleven met commerciëlere bedrijven voor een op maat gemaakte ervaring zoals we hebben gezien sinds de grote doorbraak van smartphones en sociale media. Dus hebben bedrijven ook nog nooit eerder met zoveel gegevens om moeten gaan – deze ontwikkeling staat dan ook nog relatief in de kinderschoenen. Het is nog geen 15 jaar geleden dat deze digitaliseringsgolf is begonnen, en constante innovatie drijft de ontwikkelingen steeds verder. Dat betekent ook dat er meer vraag dan ooit is naar de bescherming van privacy.

De keuze om in te investeren in digitalisering van je fitnessaanbod betekent ook dat je moet investeren in de verdere beveiliging van je klantgegevens. Hier hoef je niet zelf het wiel opnieuw voor uit te gaan vinden, of zelf expert in cybersecurity voor te worden. De eerste stap is heel eenvoudig volgens experts: dataveiligheid begint met heldere communicatie en bewustwording. Ik zie dit als een steeds belangrijker onderdeel van de positionering en propositie, specifiek voor fitnessbedrijven. Door apps en wearables krijgen clubs inzicht in steeds intiemere data over het leven van hun klanten, en daarom is het noodzakelijk om het vertrouwen van klanten te behouden in omgang met deze data.

Een goede fitness software of app biedt fitnessaanbieders de handvaten om ook daadwerkelijk data te beveiligen. Je kunt dit op meerdere manieren door bijvoorbeeld je team gebruik te laten maken van complexe wachtwoorden te gebruiken, en die ook met enige regelmaat te updaten. Goede software kan dit verplicht helpen afdwingen. Maak daarnaast gebruik van verschillende toegangsauthenticaties: als medewerkers enkel toegang hebben tot de voor hen noodzakelijke data, is de kans op problemen kleiner. Communiceer hier duidelijk over en blijf ze er ook aan herinneren, zoals je met ieder belangrijk beleid zou doen.

Dataveiligheid is dus niet alleen een belangrijk thema voor fitnessondernemers omdat de wet het voorschrijft – het is een onmisbaar voor elke club en trainer die mee wil in de golf van innovatie in de sector en goed voorbereid wil zijn op de volgende generatie van technologische ontwikkeling. Het opbouwen van een vertrouwensband tussen je merk en je klant is tenslotte minstens zo belangrijk aan de digitalisering. Als jij aan klanten laat zien dat je de veiligheid van hun gegevens serieus neemt, zullen zijn je belonen met loyaliteit.



HUGO BRAAM is technologie-evangelist in de fitnessbranche en medeoprichter van virtuagym.com, leverancier van innovatieve software voor fitnesscentra en personal trainers. hugo@virtuagym.com