Mobitwin slachtoffer van hacking

30
mei
2024

Als erkende Mobitwin Centrale is de vervoersdienst van welzijnsvereniging OPcura aangesloten bij Mpact, een overkoepelende organisatie voor alle Mobitwin Centrales in Vlaanderen.
Door een cyberaanval bij het bedrijf Mpact in Gent ondervindt de dienstverlening van Mobitwin problemen. Mpact is verwerkingsverantwoordelijke van het boekingssysteem waar onder andere Mobitwin gebruik van maakt.

Gevolgen voor de vervoersdienst OPcura:
Het systeem waarin alle ritten werden geregistreerd, is niet meer toegankelijk. Wij hebben dus geen zicht meer op reeds aangevraagde ritten, of hiervoor al een chauffeur werd vastgelegd en welke aanvragen nog openstaand zijn.

Hulplijn:
Onze chauffeurs krijgen geen automatische herinnering meer voor hun geplande ritten. Sta je toch te wachten op een chauffeur die niet komt opdagen? **Bel dan tijdens de kantooruren naar het nummer 052 36 59 38 of 052 36 59 40**, dan zoeken we naar een oplossing. Heb je van ons of de chauffeur nog geen bevestiging gekregen van een aangevraagde rit, contacteer ons dan zeker op voorhand zodat wij bij onze chauffeurs nog eens kunnen nagaan of deze rit al dan niet werd toegekend aan een chauffeur.

Nieuwe aanvragen gaan wij manueel verwerken en niet via de software van Mpact tot zolang de gevolgen van deze cyberaanval niet opgelost worden bij Mpact.

Vertel het verder:
Ben je zelf geen gebruiker van Mobitwin, maar ken je wel iemand die klant is, dan vragen we je deze persoon te verwittigen over de problemen. Zo blijft er niemand in de kou staan.

Wees waakzaam:
De impact van de hackaanval bij Mpact is nog onduidelijk, maar het is mogelijk dat jouw gegevens gelekt zijn. Als je gegevens in handen vallen van personen met slechte bedoelingen, zijn de twee grootste risico's phishing en identiteitsfraude:

Phishing:
Het per e-mail hengelen naar informatie door criminelen wordt phishing genoemd. Via de mail (maar ook via de telefoon of brief) lijken betrouwbare instanties zoals een bank of creditcardmaatschappij te vragen om bijvoorbeeld inloggegevens, creditcardinformatie, pincode of andere persoonlijke informatie. Ga hier nooit op in. Als je verdachte mails of berichten ontvangt, stuur ze dan best door naar verdacht@safeonweb.be.

Identiteitsfraude:
Bij identiteitsfraude maakt iemand misbruik van je persoonlijke gegevens. Onder je naam worden er producten of

diensten besteld, uitkeringen of creditcards aangevraagd, betalingen gedaan of bankrekeningen geopend. De fraudeur maakt zich schuldig aan oplichting en diefstal. Dit is strafbaar. Identiteitsfraude kan ernstige gevolgen hebben. Als je vermoedt dat je het slachtoffer bent van identiteitsfraude, dan doe je best aangifte bij de politie.

Wat kan ik doen om mezelf te beschermen?
Blijf alert als men je vraagt om persoonlijke data door te geven, vooral als je boodschappen ontvangt van instanties die je niet verwacht. Neem in dat geval eerst rechtstreeks contact op met deze instantie om misverstanden te vermijden. Daarnaast vind je op www.Safeonweb.be heel wat tips rond cyberveiligheid. Deze kan je altijd toepassen om de beveiliging van jouw gegevens te verbeteren, ook als er geen gegevens gestolen zijn.

Wij betreuren het feit dat Mpact slachtoffer werd van deze cyberaanval en vinden het vervelend dat wij geen toegang meer hebben tot hun software waardoor aangevraagde ritten mogelijks niet uitgevoerd worden. Wij proberen alleszins om onze werking draaiende te houden en hopen dat de problemen bij Mpact spoedig opgelost kunnen worden.

Heb je vragen over dit bericht?
Aarzel niet om ons te contacteren zodat wij een antwoord kunnen geven op al jouw vragen.