Manipulált dokumentumra hivatkozott cikkében a hvg.hu

2019. július 11. csütörtök, 17.11 / Utolsó módosítás: 2019. július 11. csütörtök, 17.11

Nem lehet ingyen vonatjegyet vásárolni a MÁV-START online rendszerén keresztül, a felhasználók adatai biztonságban vannak

Múlt hét pénteken a hvg.hu oldalon hamis információk jelentek meg, melyek szerint a MÁV-START online rendszerén keresztül lehetőség van „ingyen menetjegy vásárlásra”, illetve a felhasználók adatai veszélyben vannak. A hvg.hu manipulált dokumentumra hivatkozott, félrevezető állításaival ellentétben nem érkezett korábban bejelentés a vélt hibáról a vasúttársaság felé, valamint tömeges adatszivárgás sem történt.

A cikk állításaival ellentétben sem a MÁV Zrt-hez, sem a MÁV START-hoz nem érkezett be a hvg.hu által meghivatkozott e-mail, melyben egyik olvasójuk februárban jelezte a vélt hibát. A bejelentések megtörténtét a csatolt képernyő-fotókkal vélték bizonyítani, amelyek meglátásunk szerint azonban manipuláltak, és sajnálatosan azok hitelességét a hvg.hu szerintünk nem ellenőrizte elég pontosan. *(A képeket eredeti formájukban közöljük, amelyekből – többek között – nem derül ki az elküldés napja sem.)* Ezúton is kérjük a hvg.hu-t, hogy az olvasóközönség előtt egyértelműen vonja vissza bizonyítatlan állítását, mivel ennek elmaradása esetén a MÁV Zrt. kénytelen megtenni a szükséges jogi lépéseket.

A hvg.hu állításával szemben fizetés nélkül érvényes jegyet nem lehet generálni a MÁV-START internetes jegyvásárlási felületén keresztül. Az egyik hírben megjelenő videóban látható módszerrel, a felvétel készítője egy korábbi sikeres, fizetett vásárlás után generált menetjegy QR-kódját használta fel újra. Az ilyen módon előállított jegy nem más, mint hamis jegy, ami egyben alappal veti fel az okirat-hamisítás büntetőjogi következményeit is.

Új jegy azonban a háttérrendszerben, adatbázisban ilyenkor nem jön létre: a vonalkódban tárolt információ eltér a jegy felső részére nyomtatott adatoktól (dátum/idő, viszonylat, kedvezmények), ezért a jegyvizsgálói mobilkészülékre telepített ellenőrző alkalmazás az online jegyellenőrzés alkalmával jelzi a jegyvizsgálónak, hogy érvénytelen jegyről van szó. Ugyan egy kivezetés előtt álló informatikai rendszerről van szó, de a vasúttársaság kijavította a hibát.

A hvg.hu hamis állításával ellentétben a vásárlók elmentett adatai biztonságban vannak, azokból személyes adat kinyerése nem lehetséges.

Biztonsági hiba az ejegy rendszerben

[redacted]

at 10:42 pm Details

Expires in 0 days 4 hours 52 mins 29 seconds

Tisztelt Cím!

A https://jegyvasarlas.mav-start.hu/eTicketV2/ címen az alábbi két ***kritikus hibát*** találtam:

1, Az utazás kiválasztása után, de még fizetés előtt már létrejön a "rendelés azonosító" (REN_id). **Ezután tovább lépve a fizetés pontra, de azt NEM teljesítve, egy külön oldalon az alább említett URL-t kiegészítve, fizetés nélkül tudunk utazásra is alkalmas pdf-et (jegyet) "generálni". A jegy kijelentkezés után is a rendszerben marad.**

Az információkkal kiegészítendő URL:

https://jegyvasarlas.mav-start.hu/eTicketV2/HomePrintingTicket?REN_specazon=XXXXXXXXXX&User_ID=XXXXXXX&REN_id=XXXXXXXX

---

2. **A rendszerben lévő ÖSSZES jegyhez bárki hozzáférhet akinek van felhasználó fiókja és be van jelentkezve.** Ez azt jelenti, ha valaki automatizálja a folyamatot, gyakorlatilag a rendszerben lévő összes megvett jegyhez hozzáférhet, benne az **utasok személyes adataival(születési idő, kedvezményre való jogosultságok, pl. fogyatékosság)**.

Példa:
"A" megvesz egy jegyet.
"B" bejelentkezik.
"B", amennyiben tudja az "A"-hoz tartozó "User_ID"-t és "REN_id"-t, letöltheti a jegyét.

Úgy gondolom a leírtak alapján (főleg a 2. pontban szereplő, személyes adatok nem megfelelő védelme miatt), indokolt a szolgáltatás átmeneti felfüggesztése a hibák elhárításáig, és a felhasználók tájékoztatása az esetleges személyes adatok kikerüléséről.

Jelen levelem segítő szándékkal készült, a hibák megtalálásából semmilyen hasznom nem származott.

A hibákat, amennyiben érdemi visszajelzést nem kapok, 2019.02.19-én nyilvánosságra hozom, a felhasználók érdekében.

Üdvözlettel,

[redacted]

Reply Reply All Forward

Biztonsági hibák az eTicket rendszerben

at 10:10 pm Details

Kedves Cím!

Mivel az egy hete a helpdesk@mav-szk.hu címre küldött levelemre nem jött válasz, ezért megpróbálom itt jelenteni még egyszer.

A https://jegyvasarlas.mav-start.hu/eTicketV2/ címen az alábbi két **kritikus** hibát találtam:

1, Az utazás kiválasztása után, de még fizetés előtt már létrejön a "rendelés azonosító" (REN_id). **Ezután tovább lépve a fizetés pontra, de azt NEM teljesítve, egy külön oldalon az alább említett URL-t kiegészítve, fizetés nélkül tudunk utazásra is alkalmas pdf-et (jegyet) "generálni"(Vagy szimplán egy POST requestet használva). A jegy kijelentkezés után is a rendszerben marad. A hiba elméletben azt is lehetővé teszi, hogy valaki, az összes jegyet megvegye egy vonatra.**

Az információkkal kiegészítendő URL:

https://jegyvasarlas.mav-start.hu/eTicketV2/HomePrintingTicket?REN_specazon=XXXXXXXXXX&User_ID=XXXXXXX&REN_id=XXXXXXXX

2, **A rendszerben lévő ÖSSZES jegyhez bárki hozzáférhet akinek van felhasználó fiókja és be van jelentkezve.** Ez azt jelenti, ha valaki automatizálja a folyamatot, gyakorlatilag a rendszerben lévő összes megvett jegyhez hozzáférhet, benne az **utasok személyes adataival(születési idő, kedvezményre való jogosultságok, pl. fogyatékosság).**
Példa:

"A" megvesz egy jegyet.
"B" bejelentkezik.
"B", amennyiben tudja az "A"-hoz tartozó "User_ID"-t és "REN_id"-t, letöltheti a jegyét.

Az említett dolgokat az oldal, alapvetően hibás logikája teszi lehetővé(pl. Miért tudok általam beadott adatokkal .pdf-et generálni? Miért nincs a pdf generálás a banki tranz.id-hoz kötve? stb.). Ezen "biztonsági rések" kihasználásához nem sok szakmai tudás szükséges, gyakorlatilag csak egy másik URL-t kell beírni.
Úgy gondolom a leírtak alapján (főleg a 2. pontban szereplő, személyes adatok nem megfelelő védelme miatt), indokolt a szolgáltatás átmeneti felfüggesztése a hibák elhárításáig,a NAIH- és a felhasználók tájékoztatása az esetleges személyes adatok kikerüléséről.

A hibákat, amennyiben érdemi visszajelzést nem kapok, 2019.02.20-án nyilvánosságra hozom, a felhasználók érdekében.

Tisztelettel,

Reply Reply All Forward

Budapest, 2019. július 11.

MÁV Zrt. Kommunikációs Igazgatóság

Forrás:https://www.mavcsoport.hu/mav-csoport/manipulalt-dokumentumra-hivatkozott-cikkeben-hvghu

Hivatkozások
[1] https://www.mavcsoport.hu/sites/default/files/styles/width_1260/public/upload/e-mail_1.png?itok=xcvE2r1u