Kiberbiztonsági tájékoztató

2020.04.27.

Tisztelt Felhasználó!

Az elrendelt veszélyhelyzetet kihasználó kiberbűnözők támadásai következtében már nem csak a munkahelyen, hanem az otthoni számítógéppel végzett munka (home office) során is támadás áldozatává válhat a munkavállaló, ezáltal közvetve a munkáltató védendő értékei is károsulhatnak.

A koronavírus-járvány speciális körülményeit kihasználó **kiberbűnözők** a segítő szándékra vagy éppen a félelmekre, illetve az újabb kapcsolattartási módokban járatlanságra alapozva próbálják együttműködésre rávenni a felhasználókat. Az ilyen **támadások kivédése** érdekében is különös körültekintéssel kell eljárni. Oda kell figyelni arra, hogy milyen webhelyre látogatunk, milyen elektronikus levelet fogadunk. A gyanús levelet és annak mellékletét egyáltalán megnyitjuk-e, azokon belül mire kattintunk, elindítjuk-e a csatolmányban érkező program fájlt. Kétség esetén a váratlan, ismeretlen forrásból származó üzeneteket célszerű **azonnal jelezni a HelpDesk** e-mail címén (helpdesk [KUKAC] mav-szk.hu), avagy – elektronikus levél küldés akadálya esetén – szóban a 06-1-457-9393 közcélú, illetve 01-9393 üzemi számon.

A támadások kivédése érdekében javasoljuk:

- **Ne hagyja magát** sürgetni és nyomást alá helyezni annak érdekében, hogy egy a beérkezett e-mailben található linkre alapos megfontolás nélkül kattintson. Gyanakodjon, ha ilyet olvas a tárgy mezőben: „*Ez nagyon fontos.*”; „*Ne törölje ki a levelet olvasás nélkül!*”
- **Ne fogadja el tényként** a megjelenített küldő nevét, mivel a forrásmezőben tetszőleges név is megadható. **Gyanúra adhat okot** az is, ha a hivatalosnak gondolt levél privát e-mail címről érkezik, vagy a küldő címe megtévesztésig hasonlít egy egyébként megbízható cég hivatalos e-mail címére (*helpdesk [KUKAC] mav-szk.com; mav-szk [KUKAC] noreply.hu)*.
- **Nem elég a gyorsolvasás!** Figyeljen fel a – gyakran már magyar nyelven íródott – levelekben a helyesírási és nyelvtani hibákra. Ne sajnálja az időt és energiát a folyamatosan javuló gépi fordításokban az eltérések felkutatására („*Most mar fizetni a szamlakat egyszeru es sima utat a bankkartya*”).
- **Feltétlenül ellenőrizze** a hivatkozás megfelelőségét (mielőtt rákattint egy e-mailben kapott linkre, az egérrel csupán rámutatva megtekinthető a valódi hivatkozási cím). Az adathalászlevélben feltüntetett link többnyire hasonlít az eredeti oldal címére. A felületes felhasználó a rákattintása után még a címsorban felismerheti azt, ha a várthoz képest ott más jelent meg (böngészőeltérítés).
- **Különös óvatossággal döntsön** a csatolmányban érkező fájl megnyitásáról és még inkább egy végrehajtható fájl elindításáról! Kérjen inkább támogatást, mennyiben bizonytalan, vagy gyanús körülményt észlel.
- **Figyeljen fel arra**, ha az Önnek küldött levél megszólításában nem szerepel a neve. Az általános megszólítás gyakori az adathalász levelekben.
- **Sohase adjon meg** magáról olyan adatokat, amelyekről kis körültekintéssel belátható, hogy a levélírónak vagy egy weboldalnak nem kellene azt elkérnie. Nem lehet valós oka annak, hogy pl. egy tájékoztatásra szolgáló oldal az e-mail címét, felhasználói azonosítóját, jelszavát kérje. Ha kétségei merülnek fel, ne adja meg adatokat.
- **Ne töltsön le** mobil telefonjára az új koronavírussal kapcsolatos fontos információk közlését ígérő alkalmazást, amely valójában zsarolóvírust telepítő applikáció lehet. Szintén ne töltsön le megbízhatatlan, ellenőrizetlen forrásból származó vírus terjedését mutató online térképet, ugyanis azon keresztül is történhet káros kód terjesztése.
- **Haladéktalanul változtassa meg** a jelszavát, ha azt egy nem megbízható oldalon adta meg vagy e-mailben elküldte.
- **Ne használjon** a vállalati belépéssel **azonos vagy hasonló jelszót** internetes oldalon, mert valamely kevésbé védett szolgáltatás feltörésével megszerzett azonosítót a csaló felhasználhatja a munkahelyi fiókjába történő illetéktelen belépéshez.

- **Különös körültekintéssel járjon el** a pénzügyi adatok kezelése, továbbítása esetén. Akár ellenőrző telefonhívás és a partnerrel egyeztetett más bevett kapcsolattartási módszert is alkalmazva győződjön meg a küldő személyének azonosságáról és az üzenet tartalmának hitelességéről, amelyhez ne a kérdéses e-mailben szereplő telefonszámot vagy más elérhetőséget vegye alapul.
- Kérjük, **ismerje meg a Felhasználók biztonsági kötelezettségeit**, amelyet a MÁV intranet odalán [1] és az Informatikai Biztonsági Szabályzat 1. számú mellékletében is megtalál**.**
- **Kísérje figyelemmel** a HelpDesk biztonságos rendszerhasználatra vonatkozó hírleveleit, tartsa be a biztonság fokozása érdekében leírt intelmeket.

Mindenképpen szükséges az **Ön biztonságtudatos közreműködése** is ahhoz, hogy a MÁV informatikai rendszere továbbra is biztonságos és használható maradjon.

Köszönjük együttműködését!

MÁV Zrt. Biztonsági főigazgatóság Információ- és adatvédelem

Letölthető dokumentumok	Méret	Dátum
FELHASZNÁLÓK INFORMÁCIÓBIZTONSÁGI KÖTELEZETTSÉGEI [2]	427.27 KB	2020.04.22.

Forrás:https://www.mavcsoport.hu/kiberbiztonsagi-tajekoztato

Hivatkozások
[1] https://intranet.mav.hu/szabalyzat/ibsz/SitePages/Kezd%C5%91lap.aspx [2] https://www.mavcsoport.hu/sites/default/files/upload/page/ibsz_1_melleklet.pdf