



HÁTTÉRANYAG SZAKMABELIEKNEK • KUTATÁSI VÁLTOZAT v1 • KIADVA: 2026. OKTÓBER 22.

A csaló tudja, mit vettél kedden

Kifli.hu: ügyfélszolgálati adatszivárgás és a rá épülő célzott csalás kockázata

AI-csapattal készült, átnézte: Péter • a tények 2026. október 22-i állapot szerint

Összefoglaló

A Kifli.hu 2026. október 5-én jogosulatlan hozzáférést és adatletöltést észlelt az ügyfélszolgálati rendszerében; ugyanakkor a cseh anyacégnél, a Rohlík.cz-nél is hasonló incidens történt. Kikerülhettek az ügyfélszolgálati e-mailek, chatek, hívásátiratok, a bennük szereplő elérhetőségek, címek, rendelésszámok, kosáradatok és az AI-asszisztens feljegyzései; az érintettek száma és a behatolás módja nem ismert. A fő kockázat a kiszivárgott valódi részletekre épülő, személyre szabott csalás. A legfontosabb teendő: ha a Kifli nevében keresnek, tedd le, és te vedd fel velük a kapcsolatot a hivatalos csatornán.

Kulcsmegállapítások

- A Kifli.hu 2026. október 5-én észlelte és aznap megszüntette a jogosulatlan hozzáférést; az ügyfeleket október 11-én értesítette.
- Magyarországon a 2026. április 21. óta folytatott chatek és hívásátiratok, valamint a július 8. óta küldött e-mailek érintettek, a kosáradatokkal és az AI-asszisztens feljegyzéseivel együtt.
- A cseh Rohlík.cz-nél ugyanakkor hasonló incidens történt; ott a belépési és fizetési rendszereket kifejezetten kizárták, és bejelentették a cseh hatóságoknak.
- Az érintettek száma, a behatolás módja és a tettes nem ismert; október 22-ig nincs nyilvános hír tényleges csalási hullámról.
- Az ügyfélszolgálati rendszer a cégek egyik legértékesebb adattára: a kontextus (ki, mikor, mit rendelt) hitelesebb csalást tesz lehetővé, mint egy jelszó.

Mi történt

A Kifli.hu (a cseh Rohlik csoport magyarországi online szupermarketje) 2026. október 5-én jogosulatlan hozzáférést és adatletöltést észlelt a belső ügyfélszolgálati rendszerében. A cég közlése szerint a hozzáférést még aznap megszüntette és a hibát kijavította; az érintett ügyfeleket 2026. október 11-én e-mailben értesítette. **Megerősített** (a cég ügyféllevele, több egybehangzó sajtóbeszámoló: [Index](#), [Infostart](#), [Portfolio](#), [Origo](#)).

Ugyanezen a hétvégén a csoport cseh cége, a Rohlík.cz is bejelentette, hogy az ügyfélszolgálati eszközéből adatokat töltöttek le ([Forbes Česko](#), [Aktuálně.cz/ČTK](#)). A magyar beszámolók szerint „a vizsgálat feltárta” a magyar ügyfelek lehetséges érintettségét is ([Infostart](#), [Világgazdaság](#)). Hogy a két eset ugyanaz a behatolás-e, azt a cég nyilvánosan nem mondta ki; az időzítés és a leírás azonossága erre utal. **Feltételezés.**

Mi kerülhetett ki (Magyarország, a cég levele alapján):

- az ügyfélszolgálatnak küldött e-mailek 2026. július 8. óta;
- a chatbeszélgetések és a telefonhívások átíratái 2026. április 21. óta, a munkatársakkal és a virtuális asszisztenssel folytatottak egyaránt;
- a beszélgetésekhez feltöltött fájlok;
- a bennük szereplő nevek, e-mail-címek, telefonszámok, kézbesítési címek, rendelésszámok;
- a kosárba nemrég betett vagy onnan kivett termékek adatai;
- a virtuális asszisztens rövid feljegyzései.

Megerősített (Infostart, Index, Portfolio, Dívány).

Mi nem érintett: a cseh cég szerint a belépési és fizetési rendszerek nem sérültek, az alkalmazás és a webshop normálisan működik ([Forbes Česko](#), [Aktuálně.cz](#)). A magyar közlés ezt nem mondja ki ilyen formában, csak azt, hogy ügyfélszolgálati rendszerről van szó, nem a teljes vásárlói adatbázisról.

Jelentett (Magyarországra).

Mi nem ismert: az érintettek száma (sem Magyarországon, sem Csehországban nem közölték), a behatolás módja, az, hogy saját fejlesztésű vagy külső szolgáltató eszközéről van-e szó, és hogy ki áll a támadás mögött.

Idővonal

Dátum	Esemény	Forrás
2026. április 1.	A cseh érintett chatbeszélgetések kezdete (CZ)	czechcyber.tv , Mobilizujeme – jelentett
2026. április 21.	A magyar érintett chatek és hívásátíratok kezdete (HU)	Infostart, Index – megerősített
2026. július 8.	A magyar érintett ügyfélszolgálati e-mailek kezdete (HU)	Infostart, Portfolio – megerősített
2026. október 5.	A cég észleli a jogosulatlan hozzáférést és adatletöltést, aznap megszünteti	Infostart, Origo, Index – megerősített
2026. október 11.	Ügyféllevél Magyarországon és Csehországban; magyar sajtóbeszámolók (HVG nyomán)	Infostart, Origo, Mobilizujeme – megerősített
2026. október 11–12.	A cseh cég bejelenti az esetet a cseh kiberbiztonsági (NÚKIB) és adatvédelmi hatóságnak (ÚOOÚ)	Forbes Česko, Aktuálně.cz, Expats.cz – megerősített
2026. október 22.	Nincs nyilvános hír tényleges csalási hullámról, hatósági eljárásról vagy az érintettek számáról	saját keresés – jelentett

Szereplők és háttér

- **Kifli.hu:** online élelmiszer-kereskedő, a cseh Rohlik csoport tagja ([Economx](#)). Az Origo szerint 2024-ben a második legnagyobb hazai online kereskedő volt.
- **Rohlik csoport:** cseh online supermarket, több országban működik (Németországban Knuspr néven). A cseh cégnél szintén ügyfélszolgálati adatok szivárogtak ki; más piacokról (Németország, Ausztria stb.) nincs nyilvános beszámoló. **Jelentett.**
- **Előzmény, minta:** az ügyfélszolgálati rendszer mint célpont nem új. 2025. október 3-án a Discord jelentette be, hogy egy külső ügyfélszolgálati partnerén keresztül a támogatási beszélgetésekhez és

mintegy 70 000 felhasználó személyazonosító fotójához fértek hozzá, és a támadók váltságdíjat követeltek ([Discord](#), [Bitdefender](#)). Az Origo szerint a hazai online kiskereskedelembe ilyen kiterjedésű ügyfélszolgálati incidensre nincs dokumentált előzmény.

Hogyan működik (Red // támadói szemmel)

- **Az ügyfélszolgálat a cég „naplója”.** Ide írja le az ügyfél, mi hiányzott a csomagból, mikor rendelt, hova kéri a szállítást – és néha olyat is, aminek nem itt lenne a helye (jelszó, kártyaadat). A cseh cég maga is jelezte, hogy egyes ügyfelek jelszót vagy kártyaadatot is megosztottak a beszélgetésekben, őket külön értesítette ([Expats.cz](#)).
- **A kontextus az érték, nem a jelszó.** A csaló a valódi részletekből (rendelészám, hiányzó termék, korábbi panasz, kosártartalom) hiteles ürügyet épít: visszatérítés, ügyfélszolgálati visszahívás, „gyanús belépés” miatti kódkérés. Erre maga a cég figyelmeztetett: a csalók az ügyfélszolgálatnak vagy visszatérítést intéző munkatársként adhatják ki magukat ([Dívány](#)).
- **A virtuális asszisztens is adattár.** Az AI-asszisztens feljegyzései összefoglalják, mit akart az ügyfél – a támadónak ez kész forgatókönyv.
- **A trükk pszichológiai.** A valódi részlet kikapcsolja a gyanút, a sürgetés pedig nem hagy időt gondolkodni.

Hatás és magyar vonatkozás

- **Közvetlen érintettek:** a Kifli.hu ügyfelei, akik 2026. április 21. óta chaten vagy telefonon, illetve július 8. óta e-mailben kapcsolatba léptek az ügyfélszolgálattal. Számuk nem ismert.
- **Közvetett kockázat:** személyre szabott adathalász e-mailek, SMS-ek és hívások a cég nevében, akár hetekkel-hónapokkal később is. A cég maga figyelmeztet erre.
- **Hatóság:** a cseh cég a cseh hatóságoknak bejelentette az esetet. Magyar hatósági (NAIH) bejelentésről vagy eljárásról nyilvános információ nincs; a GDPR szerint a súlyos incidenst 72 órán belül a felügyeleti hatóságnak is be kell jelenteni, ezért valószínű, de nem megerősített. **Nyitott.**
- **Csalási hullám:** 2026. október 22-ig nincs nyilvános beszámoló tényleges, a kiszivárgott adatokra épülő csalási hullámról. **Jelentett (hiány).**

Mit tegyél (Blue // mit tegyél most)

Magánszemély (Kifli-ügyfél):

1. Ha a Kifli nevében hívnak vagy írnak, tedd le / ne válaszolj, és az alkalmazásból vagy a kézzel beírt kifli.hu címen vedd fel velük a kapcsolatot.
2. Üzenetben kapott linkre ne kattints, és ne telepíts semmit visszatérítés ürügyén.
3. Soha ne adj meg jelszót, netbanki adatot, kártya biztonsági kódját vagy SMS-kódot kéretlen hívásra vagy üzenetre.
4. Ha valaha jelszót írtál az ügyfélszolgálatnak, cseréld le – mindenhol, ahol ugyanazt használod.
5. Ha banki adatot adtál meg, azonnal szólj a bankodnak.
6. Szólj a szüleidnek, nagyszüleidnek: ők kapják a legmeggyőzőbb hívásokat.

Kisvállalkozás (webshop, szolgáltató):

1. Nézd meg, mit tárol az ügyfélszolgálati rendszered (chat, e-mail, hívásátírat), és mennyi ideig – állíts be megőrzési időt.
2. Kapcsold be a kártyaszám- és jelszómintázatok automatikus maszkolását, ha a rendszer tudja.
3. Írd le az ügyfeleidnek nyíltan: „így keresünk, és így soha”.
4. Kérdezd meg a szolgáltatót, ki fér hozzá a rendszerhez (munkatársak, külsős partnerek, AI-integrációk).

Szervezet:

1. Kezeld az ügyfélszolgálati platformot (ticketing, chat, hívásrögzítés, AI-asszisztens) kiemelt adattárként: hozzáférés-kezelés, MFA, naplózás, anomálfigyelés.
2. Adatminimalizálás: rövid megőrzési idő, maszkolás, az érzékeny adat kivezetése.
3. Szállítói kockázat: a külső ügyfélszolgálati partnerek és integrációk hozzáféréseinek rendszeres felülvizsgálata, gyors visszavonhatóság.
4. Incidenskommunikációs sablon: konkrét „így keresünk / így nem” mondatokkal, a hivatalos csatornák megnevezésével.

Szakmai blokk

- **CVE / érintett termék:** nem ismert; a cég nem nevezte meg sem a rendszert, sem a sérülékenységet.
- **Valószínű MITRE ATT&CK technikák (a következményekre, nem a behatolásra):** T1598 / T1566 (adathalászat a kiszivárgott kontextussal), T1656 (megszemélyesítés). A behatolás technikája nem ismert.
- **Észlelési ötletek (ügyfélszolgálati platformokra):** tömeges export vagy API-lekérdezés figyelése, szokatlan időpontú vagy helyről érkező ügynöki belépés, új integrációs token vagy alkalmazás, nagy mennyiségű csatolmány-letöltés.
- **Hivatalos ajánlások:** a cég ajánlásai (lásd Blue). A cseh hatóságok (NÚKIB, ÚOOÚ) bejelentést kaptak, nyilvános ajánlást nem tettek közzé az esetről.
- **Indikátorok:** nincsenek nyilvánosan közölve.

Ellentmondások és nyitott kérdések

- **Eltérő időszakok:** a cseh beszámolók szerint ott a chatek 2026. április 1. és október 5., a hívásátíratok április 28. és október 5., az e-mailek június 28. és szeptember 22. közöttiek; Magyarországon április 21. (chat, hívás) és július 8. (e-mail) óta. A különbség oka nem ismert (eltérő bevezetés, eltérő megőrzés?).
- **Egy vagy két incidens?** Nem mondták ki, hogy a magyar és a cseh eset ugyanaz a behatolás.
- **Belépés és fizetés:** Csehországban kifejezetten kizárták az érintettségét, Magyarországon ilyen mondat nem jelent meg.
- **Érintettek száma, behatolás módja, külső szolgáltató szerepe, tettes:** nem ismert.
- **Magyar hatósági bejelentés:** nincs róla nyilvános információ.
- **Tényleges csalások:** október 22-ig nincs róluk nyilvános beszámoló.

Forrásértékelés

Forrás	Típus	Megbízhatóság	Mit támaszt alá
Infostart	sajtó (a cég közleménye alapján)	magas	dátumok, adatkörök, ajánlások
Index	sajtó	magas	dátumok, adatkörök, ajánlások
Portfolio	sajtó (HVG nyomán)	magas	adatkörök, ügyféllevél
Origo	sajtó	közepes	dátumok, piaci pozíció, előzmény hiánya
Dívány	sajtó	közepes	a cég figyelmeztetése a megszemélyesítésről
Világgazdaság	sajtó	közepes	magyar érintettség a vizsgálat nyomán
Forbes Česko	sajtó (ČTK, céges nyilatkozat)	magas	cseh eset, hatósági bejelentés, belépés/fizetés nem érintett
Aktuálně.cz	sajtó (ČTK)	magas	céges nyilatkozatok, hatóságok
Expats.cz	sajtó	közepes	jelszót/kártyaadatot megosztók külön értesítése
czechcyber.tv	szaksajtó	közepes	cseh időszakok
Mobilizujeme	sajtó	közepes	cseh időszakok, kosáradatok
Brandsit	sajtó	közepes	AI-asszisztens feljegyzései
Economx	háttér	közepes	Rohlik anyacég
Discord	cég	magas	előzmény: ügyfélszolgálati partneren át
Bitdefender	kutató/sajtó	közepes	Discord-előzmény számai