információbiztonsági tudnivalók - CEO fraud és deepfake

Kedves Imre!

A K&H vállalati biztonságtudatosság program részét képező hírlevelekben megismerheti a leggyakoribb vagy az aktuálisan legnagyobb veszélyt jelentő támadási formákat, valamint ezek kivédési módjait. A vállalatokat érintő támadások sok esetben specifikusabbak, mint azok, amelyeknek elsősorban a magánszemélyek a célpontjai, azonban a vállalatok esetén is elég egyetlen óvatlan kolléga és már meg is történik a baj. Hírlevél sorozatunkban abban próbálunk segíteni, hogy a kollégák megértsék a veszélyt, ami rájuk – és rajtuk keresztül a vállalatra leselkedik.

CEO fraud támadások

A CEO fraud (vagy más néven whaling) az adathalászat azon formája, amikor a támadók „nagy halakra” – a vállalat felsővezetőire, pénzügyi vezetőire, HR vezetőire, döntéshozóira és a felsővezetői asszisztensekre – vadásznak. Ugyan a támadás célpontjai a döntéshozók, azonban ez nem zárja ki azt, hogy a támadás során más – szintén magas pozícióban lévő – kollégát személyesítsenek meg a csalók.
A CEO fraudot leginkább az különbözteti meg az egyszerű adathalászattól, hogy **a – magas megtérülés reményében – a támadás megvalósításába fektetett munka nagyságrendileg nagyobb, sok esetben több hónapig tartó kutatómunka előzi meg**.
A CEO fraud megvalósítása előtt a támadók gondosan feltérképezik a megtámadni kívánt felsővezető személyes és szakmai profilját, tevékenységét, érdeklődési körét, munkatársait, családi és baráti hátterét, szakmai kapcsolatait. A felderítés magában foglalja a social media profilok gondos tanulmányozását, az interneten fellelhető adatok összegyűjtését, adott esetben célzott – a támadást előkészítő, információgyűjtésre

szolgáló – telefonos, vagy online csatornás megkereséseket… a lehetőségek száma végtelen.
Az összegyűjtött információk alapján **a támadók személyre szabott megkeresést indítanak, amelyet a csalók magukkal a megszerzett információkkal tesznek hitelessé**.

- a megkeresések tökéletes nyelvezetűek, nem tartalmaznak gépelési, helyesírási, nyelvtani hibákat, tárgyuk és tartalmuk releváns
- az esetek többségében valós, vagy a megtámadott fél által ismert személy nevében készülnek (vö. BEC típusú támadások)
- az e-mailek csatolmányt, vagy olyan linket tartalmaznak, amiről nehezebb kideríteni, hogy valójában hova mutat (pl. bit.ly stb.)
- amennyiben üzleti típusú a megkeresés, az jó – de nem feltűnően jó – ajánlat lehetőségét lebegteti meg.

Fontos tudni, hogy **bizalmi munkakörük és tág jogosultsági szintjük miatt a CEO fraud támadások a felsővezetői/személyi asszisztenseket is érintik**.

a deepfake technika

A CEO fraud típusú támadások másik fő csatornái a hang-, vagy videókommunikációt lehetővé tevő csatornák (telefon, csevegő alkalmazások). Az így megvalósított támadások azért különösen veszélyesek, mert a csalók egyre több esetben deepfake technológiát használnak a megvalósítás során: miután megszületett a támadási forgatókönyv, aminek része, hogy meghatározzák, hogy a döntéshozó mely kapcsolatát kívánják megszemélyesíteni, a támadók képeket, rövid videókat töltenek le a publikus internetről és ezeket felhasználva létrehoznak egy olyan – deepfake – személyt, aki pontosan ugyanúgy néz ki és pontosan ugyanolyan a hangja, mint annak a személynek, akinek a nevében fel szeretnék venni a kapcsolatot. A támadók ezeken deepfake-kel létrehozott személyeken keresztül valós időben – nem előre rögzítetten – kommunikálnak, reakcióikat, válaszaikat a megtámadott fél reakcióihoz tudják igazítani.

a CEO fraud elleni védekezés

- Hasonlóan a célzott adathalászat elleni védekezéshez, a CEO fraud típusú csalásoknál is fontos, hogy a legkisebb gyanú esetén is **ellenőrizzük a kapcsolatot egy másik csatornán** (pl. telefonon, az általunk ismert telefonszámot felhívva).
- Legyünk tudatában annak, hogy **minden, amit a publikus internetre feltöltöttünk, felhasználható**. Akár információgyűjtésre, ami alapján célzott támadást kaphatunk, akár arra, hogy visszaéljenek fényképeinkkel, videóinkkal, hanganyagainkkal, felhasználják jellegzetes stílusunkat, gesztusainkat,

szófordulatainkat. **Különítsük el egymástól céges és magánéleti tevékenységünket, próbáljuk megnehezíteni a csalók dolgát.**

- Javasolt a **tudás alapú hitelesítési metódus** bevezetése, ami azonban nem PIN-kódot, vagy előre meghatározott jelszót jelent, hanem a helyzethez rugalmasan alkalmazkodó vagy történet alapú megközelítést pl. ha biztosak vagyunk abban, hogy az elmúlt időszakban nem utaltunk a másik félnek, akkor az „Ugye megkaptátok tegnap az x Ft-ot, amit átutaltunk?” kérdés helyénvaló lehet, ugyanis ha a válasz „Igen”, vagy „Nem”, akkor tudhatjuk, hogy nem az igazi partnerrel beszélünk, hiszen ő nem is vár tőlünk teljesítést. Fontos, hogy ezek az ellenőrző kérdések valóban **ne előre meghatározott kérdések legyenek, hanem az adott helyzethez alkalmazkodjanak és minden esetben kontextus alapúak** legyenek.
- A **négy-, vagy több-szem elv – mint folyamatba épített ellenőrzés** – további kontrollt biztosít a csalásokból származó károk megelőzése érdekében. Ekkor egymástól több (legalább 2), független személy ellenőrzi az átutalásokat, könnyebben észrevehetőek a hibák, tévedések.

banki támogatás a védekezéshez

K&H Electrában meghatározhatja számlánként, hogy a megbízások jóváhagyására egyes (tól-ig) összegsávok közötti megbízások esetén a felhasználóktól hány aláírási pontot vár el, azaz a pontszámok segítségével szabályozhatja, hogy hány aláíró szükséges a megbízás elindításához.

Javasoljuk, hogy a felhasználói aláírási limit pontszámokat úgy alakítsa ki, hogy **lehetőleg több felhasználó közreműködése legyen szükséges egy megbízás elindításához**. Pl. egy 10 pontos felhasználó helyett javasolt két 5-5 pontos felhasználót bevonni a folyamatba, mivel a csalás kockázata csökkenthető független személyek közreműködésével

Amennyiben minden megbízásra vonatkozóan ez napi működését korlátozná, akkor javasoljuk, hogy **legalább a magasabb összegű megbízások esetén állítsa be, hogy egynél több felhasználó aláírására legyen szükség**. Beállítható például, hogy 0-1 000 000 Ft között 5 aláírási pont, 1 000 000 – korlátlan összeg értéksávban pedig 10 aláírási pont legyen az elvárt a megbízások jóváhagyásához. Ezen beállításokat megteheti a beállítások/jogosultságkezelés/aláírási limitek menüpontban.

kapcsolódó tartalmak:

- a deepfake veszélye – podcast epizód
- kiberbiztonsági hírlevelek korábbi részei
- általános információkat a K&H Bank Biztonság a pénzügyekben oldalán találhat

Üdvözlettel:
K&H Bank

Vállalati Ügyfélszolgálat +36 1 468 7777 » kh.hu » bank@kh.hu a KBC Csoport tagja

Ezt a levelünket a(z) imre.fonai1@gmail.com címre küldtük.

Leveleinket minden esetben a K&H Bank hivatalos domain-jéről küldjük, tehát a feladó e-mail címében **a @ utáni rész utolsó két tagja minden esetben kh.hu**. Leveleink csak kh.hu aloldalaira mutató linket tartalmaznak, azaz, ha a link fölé húzza az egérkurzort, az ablakban megjelenő link címének első része minden esetben kh.hu, vagy cdn-exponea.kh.hu.

Az adathalászat komoly fenyegetést jelent mindenki számára. A támadó bármilyen online csatornán, de SMS-ben, vagy épp telefonon is megkeresheti. A K&H Bank soha nem kezdeményez telefonhívást a +36 1/20/30/70 335-3355 telefonszámok bármelyikéről**, ezeket a számokat kizárólag ügyfelek telefonhívásainak fogadására tartja fenn**. Amennyiben az előbbi számok bármelyikét látja a kijelzőn, telefonszám hamisításos csalás áldozatává válhat, ezért ilyen esetekben kérjük, hogy haladéktalanul szakítsa meg a vonalat. Kérjük, hogy mielőtt az adatait kiadná, győződjön meg arról, hogy a kapcsolatot felvenni szándékozó személy vagy szervezet az, akinek mondja magát és soha ne kattintson gyanús üzenetben érkező linkre, vagy csatolmányra.

KiberPajzs
Védelem a pénzügyekben

Vértezze fel magát a kibercsalásokkal szemben, látogasson el a KiberPajzs honlapra! (https://kiberpajzs.hu)
További információkat a https://www.kh.hu/biztonsag-a-penzugyekben oldalon talál.
Ügyeljen adatai biztonságára!

Jelen üzenetet a K&H Bank Zrt. (1095 Budapest, Lechner Ödön fasor 9., a továbbiakban: Bank), mint adatkezelő korábban adott hozzájárulása alapján küldte meg Önnek a részére megadott elektronikus levelezési címére.

Hozzájárulását kifejezetten erre a programra vonatkozóan bármikor, korlátozás és indokolás nélkül, ingyenesen visszavonhatja a bubadigi@kh.hu elérhetősége felé intézett nyilatkozattal. Hozzájárulás visszavonása hiányában a Bank a regisztráció során megadott adatait a program végét követően, legkésőbb 2025. év végén törli.

Az adatkezeléssel kapcsolatos bővebb tájékoztatást a https://www.kh.hu/adatvedelem internetes oldalon található Adatkezelési tájékoztatóban, valamint a Bank Üzletszabályzatában talál, továbbá személyes adatai kezeléséről tájékoztatást kérhet a Bank Vállalati Ügyfélszolgálatán (+36 1 468 7777, vallalatiugyfelszolgalat@kh.hu).

Jelen üzenet nem minősül ajánlattételnek. A kondíciók módosításának jogát a Bank fenntartja. A mobilinfo termék részletes leírását, illetve feltételeit az ügyfélszerződés, a Vállalati ügyfelek részére nyújtott pénzforgalmi és betéti szolgáltatások Általános Szerződési Feltételei, a K&H Mobilinfo szolgáltatás Általános Szerződési Feltételei, az Elektronikus azonosítású banki szolgáltatások Általános Szerződési Feltételei, az Üzletszabályzat, valamint az aktuális Hirdetmény vállalati ügyfelek részére tartalmazza, mely dokumentumok megtekinthetőek a kh.hu internetes oldalon és a K&H Bank személyes ügyfélpontjaiban.