
# információbiztonsági tudnivalók - BEC típusú csalások

## 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.

### mi az a célzott adathalászat?

A  Business Email Compromise (BEC) a támadások egy olyan fajtája, amely során a csalók jellemzően valódi üzleti email fiókokat használnak fel a csalásokhoz.
Az egyszerű adathalászathoz képest a legnagyobb különbség, hogy a BEC típusú támadások nagyon sok esetben a támadáshoz a partner cég valódi domainjét használják fel, amit megszerezhetnek például egy felhasználói fiók feltörésével, vagy akár a céges levelezés meghamisításával. Ilyen esetben a támadás egy létező, érvényes címről érkezik, így a felismerése nagyon nehéz. A BEC típusú támadások célja lehet a pénzügyi haszonszerzés, az adatlopás, vagy akár az üzleti folyamatok ellehetetlenítése.
A BEC típusú támadások jellemző célpontjai a vállalatok felsővezetői, pénzügyi vezetői, HR vezetői, esetleg a pénzügyi területen dolgozó kollégák.

### a BEC típusú támadások típusai

A támadások jellemzően nagyon hasonló módszerekkel operálnak, melyek célja a teljes bizalom elnyerése oly módon, hogy valóban létező kapcsolatunknak álcázzák magukat, felhasználva akár az arculati, stílusbeli elemeket.

- **e-mail fiók feltörése:** A támadók feltörik a vállalat alkalmazottjának – rosszabb esetben vezetőjének – az email fiókját, a továbbiakban erről – a valós, de a támadók által (is) kezelt fiókról küldenek utasítást akár szenzitív adatok megosztására, vagy (hamis) számlák kiegyenlítésére, esetleg pénzösszegek utalására.
- **e-mail fiók hamisítása:** Amennyiben egy cég nem rendelkezik megfelelő biztonsági beállításokkal, az elavult protokollok miatt a cég e-mailjei meghamisíthatóak, így a csalók a céghez tartozó email címről, tetszőlegesen választott – akár létező - kolléga - nevében küldhetnek e-maileket úgy, hogy nem szükséges az e-mail fiókot feltörniük.
- **Fake Invoice Scam:** a támadók a vállalat egyik üzleti partnerének a nevében küldenek hamis számlá(ka)t, amelyek úgy tűnnek, mintha a valódi beszállítóktól érkeztek volna. A családhoz a támadók feltörhetik, vagy meghamisíthatják a beszállító email fiókját.

A BEC típusú támadások esetén mindig érdemes szem előtt tartanunk, hogy nem pusztán elszenvedői, de „elkövetői” is lehetünk ezeknek a támadásoknak oly módon, hogy az általunk képviselt vállalat nevében követnek el támadást, ami az elhúzódó jogi procedúrán túl akár reputációs kárt is okozhat vállalatunknak.

## vállalatok és a BEC elleni védekezés

Hasonlóan a célzott adathalászat elleni védekezéshez, a BEC típusú csalásoknál is fontos, hogy a legkisebb gyanú esetén is ellenőrizzük a feladót egy másik csatornán (pl. telefonon, az általunk korábbról ismert telefonszámot felhívva).

A **kétfaktoros (vagy többfaktoros) azonosítás** komoly védelmet nyújt a postfiókok feltörése ellen. A többfaktoros azonosítás (2FA, vagy MFA) során a támadónak nem elegendő a postafiókhoz tartozó jelszót (tudás alapú) megszereznie, de egy másik (birtoklás, vagy tulajdonság alapú) faktort is meg kell szereznie annak érdekében, hogy hozzáférjen levelezésükhöz.

A **négy-, vagy több-szem elv – mint folyamatba épített ellenőrzés** – további kontrollt biztosít a csalásokból származó károk megelőzése érdekében. Ekkor egymástól függetlenül több (legalább 2), független személy ellenőrzi az átutalásokat, emiatt könnyebben észrevehetőek a hibák, tévedések.

A **levelezéshez tartozó domainek megfelelő konfigurációja** szintén megakadályozhatja, vagy csökkentheti a BEC típusú támadások előfordulását: a

megfelelő SPF, DKIM és DMARC beállítások megóvják a vállalatot attól, hogy a nevében arra nem jogosultak levelet küldjenek.

A megkereséseken található **minősített elektronikus aláírás** igazolja, hogy a levelet valóban az a személy küldte, akinek az aláírását látjuk. Ez egyrészt bizonyítja számunkra, hogy ténylegesen a partnerünktől érkezett megkeresés, másrészt a segítségével igazolhatjuk a másik fél felé, hogy megkeresésünk nem csalás.

kapcsolódó tartalmak:

- videó a célzott támadásokról
- K&H kiberbiztonsági ügyfélrendezvény felvétele

## banki támogatás a védekezéshez

A számlákat, dokumentumokat érdemes elektronikus aláírással ellátni, ezáltal biztosítani eredetiségüket. A banki ügyintézés során is használható már az elektronikus aláírás. A kétfaktoros belépést követően a K&H e-posta rendszerén keresztül kezelheti dokumentumait, jelentős számú ügymenet esetén azokat elektronikusan alá is írhatja tanúsítványával akár közvetlenül a felületről indítva.

További információk a K&H Bank Biztonság a pénzügyekben oldalán találhatóak.

**Üdvözlettel:**
**K&H Bank**

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

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.