A BUSINESS EMAIL COMPROMISE NÉGY LEGGYAKORIBB MÓDJA

Az álcázás nagymesterei az üzleti emailekhez kapcsolódó visszaélések

FORRÁS: NYTIMES.COM

Van, hogy a szemközti íróasztalnál ülő kolléga emailjének álcázza magát, van, amikor a hivatalos vállalati címekhez hasonló formát ölt, míg a vezetők célba vételéhez egy jól ismert munkatárs bőrébe bújik. Az üzleti emailekhez kapcsolódó visszaélések nagyon megszaporodtak a Covid-járvány kirobbanását követően, de utána sem javult a helyzet, sőt. Melyek a leggyakoribb módjai és miként lehet átlátni az átverésen?

Aggasztó számadatok, a kereskedelem, a szállítás, az informatika és a kiskereskedelem területén működő szervezetek elleni megsokszorozódott visszaélések, milliókban mérhető veszteségek. Business Email Compromise (BEC) áldozatául esik minden ötödik cég, akár hazai, akár nemzetközi piacot nézzük. Ez globálisan 3,5 milliárd dollár kárt okozott 2019-ben az FBI Internet Crime Complaint Center szerint, a tendencia pedig növekvő. A BEC alkalmazásának leggyakoribb módjait gyűjtöttük össze.

1. Megtévesztő, felső vezetői levél

A Kaspersky aktuális összefoglalója szerint a BEC leggyakoribb módja a megtévesztő, felső vezetői levél. A beosztott kap egy levelet a vezetőjétől vagy egy magasabb pozícióban lévő kollégájától, amelyben arra kérik, hogy dolgozzon együtt egy harmadik féllel (aki lehet megrendelő, ügyvéd, stb.), ami pedig bizonyos bizalmas vállalati adatokat megosztásával jár. Mivel ezek a levelek a megszólalásig hasonlítanak a valódihoz, magasabb beosztású kollégától érkeznek, akit akár személyesen is ismer a dolgozó, meg sem fordul a fejében, hogy csalásról lenne szó.

2. Volt, nincs – pénzkicsaló számla

Egyszerű, mégis „nagyszerű” trükk a pénzügyi osztálynak címzett, fizetési késedelem tárgyú levél, amely tartalmazza is a „szállító” által kiállított számlát. Sok esetben a csalók az olyan cégek képében lépnek fel, akik rendszeresen állítanak ki számlát a szervezetnek, hogy a megtévesztés nagy valószínűséggel sikerrel járjon.

3. Ajándékkártya-átverés

Ebben az esetben is vezetőnek vagy magasabb pozíciójú kollégának adja ki magát a csaló, aki levélben arra kéri meg az adott kollégát, hogy segítsen a céges vagy az ügyfélnek szánt ajándék megvásárlásában. Szintén a bizalmas adatok megszerzése a cél.

4. Bérszámfejtési átverés

Az átverés során a csaló egy, a cégnél dolgozó alkalmazott nevében levelet küld a pénzügynek, amelyben bérfizetési hitelesítő adatainak, konkrétan a bankszámla- és/vagy a bankkártyaszámának frissítését kéri. Ha ez megtörténik, akkor a következő havi bért már a csaló kapja meg.

Kiss Franciska

Három lépésben a BEC ellen

- A legjobb védekezés a megelőzés, azaz a cégeknek érdemes fejlett technológiákkal ellátott, adathalászat és levélszemét ellen is védelmet nyújtó biztonsági megoldást használni.
- A szoftveres megoldásokon túl a munkatársak digitális biztonságtudatosságának fejlesztésére is komoly hangsúlyt kell fektetni, meg kell tanítani azokat az alapvetéseket, amelyek tudatában önállóan is kiszúrják a BEC-t.
- A biztonságtudatosság másik aspektusára, a megosztásra is fel kell hívni a figyelmet: érdemes nyomatékosítani a munkavállalók számára azt, hogy ne osszanak meg széles körben túlságosan sok részletet a munkájukról, tehát a közösségimédia-platformokon ne kommunikáljanak olyan adatokat, amelyek később BEC alapjául szolgálhatnak.