információbiztonsági tudnivalók - jogosultságkezelés

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.

jogosultságokból származó veszélyek

A vállalati információbiztonság egyik alapelve, hogy minden felhasználó csak ahhoz férjen hozzá, ami a munkájához feltétlenül szükséges. Ha valaki túlzott jogosultságokat kap – például hozzáfér kritikus rendszerekhez, pénzügyi adatokhoz vagy adminisztrációs funkciókhoz, amelyek nem tartoznak a feladataihoz –, az nem csak technikai, hanem üzleti, illetve reputációs kockázatot is jelent, megnöveli az adatvesztés, vagy adatszivárgás kockázatát, megteremtheti a véletlen vagy szándékos adatmódosítás lehetőségét.

Az összeférhetetlen jogosultságok ugyanilyen veszélyesek: amikor egy személy olyan jogokat birtokol, amelyek lehetővé teszik egy folyamat teljes végrehajtását (például tranzakció rögzítése és jóváhagyása), megszűnik az ellenőrzés, nő a csalás, adatmanipuláció vagy tévedés esélye, amiből gazdasági, reputációs, vagy megfelelősségi kára származhat a vállalatnak.

legjobb megoldás a megelőzés

- **szerepkör-alapú hozzáférés**
  Kerüljük az „általános admin” szerepköröket, minden munkatárs olyan szerepkör-csoportba kerüljön, amellyel el tudja látni a feladatait anélkül, hogy más - a munkakör ellátásához nem szükséges - jogosultságokat birtokolna. Pl. a programok telepítését kizárólag a rendszergazdák végezhessék, az átutalásokat indító kollégák ne férhessenek hozzá a HR dokumentumaihoz stb.
- **jogosultságok szétválasztása**
  Kritikus folyamatoknál tiltsuk meg, hogy ugyanaz a személy vigye végig a folyamatot pl. rögzítsen és hagyjon jóvá egy tranzakciót. Ez a négy szem elv alapja.
- **rendszeres felülvizsgálat**
  Változáskor ellenőrizzük, hogy a jogosultságok megfelelnek-e az aktuális feladatoknak. Mivel a régi jogok még így is gyakran maradnak meg, érdemes évente minden jogosultságot felülvizsgálni és a szükségteleneket törölni.
- **négy szem elvű kontroll**
  Kritikus műveletekhez két (vagy több) független személy jóváhagyása szükséges. Ez csökkenti a visszaélés esélyét.
- **erős azonosítás és naplózás**
  Többfaktoros hitelesítés, erős jelszavak és naplózás segít a jogosultságok, illetve a jogosultságok segítségével elkövetett hibák/visszaélések nyomon követésében, felderítésében.
- **tudatosság és felelősség**
  Ha gyanús vagy indokolatlan hozzáférést észlelünk, azonnal jelezzük azt az információbiztonsági csapatnak.

banki támogatás a védekezéshez

K&H Electra rendszerben lehetősége van az önadminisztrációs joggal rendelkező felhasználónak a saját, és további céges felhasználóik jogainak a menedzselésére. Ezek a számla és funkciójogok megadhatók akár külön-külön az adatok megtekintésére, rögzítésre, illetve a megbízások aláírására, jóváhagyására vonatkozóan is.

kapcsolódó tartalmak

- mit tegyünk ha mégis megtörtént a baj – 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.