2020.11.20.

BIZTONSÁGI ELJÁRÁSOK

MAGYAR BANKHOLDING ZRT.

A biztonságnak pénzügyeink intézésében kimagaslóan nagy szerepe van, ezért a Magyar Bankholding Zrt. informatikai rendszerei folyamatos fejlesztés alatt állnak annak érdekében, hogy a rendszerek adatai, valamint funkcionalitásai, illetve a bennük kezelt személyes adatok megfelelő szintű védelme az egyes szolgáltatások által támasztott követelményeknek megfelelően minden esetben rendelkezésre álljanak.

Mindezeket szem előtt tartva informatikai rendszereink kialakításakor nagy teljesítményű és megbízhatóságú, korszerű informatikai és biztonsági rendszerelemekből építkezünk, amelyeket szigorú fejlesztési és üzemeltetési rend mellett alkalmazunk. Folyamatosan figyelemmel kísérjük és elemezzük az esetleges fenyegető veszélyeket annak érdekében, hogy minden esetben kockázatarányos intézkedésekkel biztosítani tudjuk rendszereink magas szintű adatvédelmét és adatbiztonságát.

Társaságunk informatikai rendszerének védelme különböző technikai eszközök használatával és szervezési intézkedések alkalmazásával valósul meg az üzleti és védelmi célok fényében, valamint többrétegű vírus- és kártékonykód védelmi megoldást is alkalmazunk. A védendő rendszereinket oly módon üzemeltetjük, amely lehetővé teszi az illetéktelen cselekmények ellenőrzését és a felelősök megállapítását. Társaságunk a rendszerek bevezetése során élesbe állítás előtt minden esetben elvégzi azok biztonsági megerősítését.

Rendszereink védelme érdekében legfontosabbnak, azok elemei és adatai funkcionalitásának, rendelkezésre állásának, bizalmasságának, integritásának, sértetlenségének, hitelességének megóvását tekintjük. Mindezek mellett kiemelt figyelmet szentelünk a hozzáférésvédelemnek, adat- és titokvédelemnek, valamint a működésbiztonságnak, és megfelelő technikai és szervezési intézkedéseket alkalmazunk ezek kikényszerítése és érvényesítése érdekében.

A szolgáltatásfolytonosságot akadályozó rendkívüli események kezelésére üzletmenetfolytonossági és katasztrófa elhárítási tervek állnak rendelkezésre, amelyeknek célja, hogy rendkívüli helyzetekben is biztosítsák a működési feltételeket.

A biztonsági kockázatokkal arányos módon az adatszivárgás kockázatának kezelésére átfogó, a potenciális csatornákat központilag felügyelő védelmi folyamatokat támogató megoldást üzemeltetünk, monitorozási intézkedéseket alkalmazunk, az esetleges adatvédelmi incidensek kezelésére pedig olyan eljárásrendet alkalmazunk, amely biztosítja, hogy az incidensek detektálása, kivizsgálása és hatásainak a csökkentése a lehető leghatékonyabb legyen.

Adat- és információbiztonsági tevékenységeink célja, hogy biztosítsák az adatok biztonságát, azaz bizalmasságát, sértetlenségét, hitelességét és rendelkezésre állását, az adat- és titokvédelem pedig biztosítja a védendő információk védelmét. A jogszabályokban meghatározott, illetve saját hatáskörünkben védendőnek nyilvánított információkat (szolgálati és államtitok, bank-, értékpapír-, pénztár-, és üzleti titok, személyes adatok, stb.) megfelelő technikai és szervezési intézkedések bevezetésével és fenntartásával védjük.

A kialakított biztonság fenntartásához elengedhetetlen az Ön közreműködése, körültekintő, elővigyázatos eljárása, és az Ön által használt eszközök magas biztonsági szintje, hogy a csalók ne kaphassanak esélyt egy sikeres támadásra.

Hasznos tanácsok banki ügyintézés során:

- Javasoljuk, hogy csak olyan körben és minőségben bocsásson adatot az ügyintéző rendelkezésére, amely alapján Önt azonosítani lehet.
- Az azonosításra szolgáló személyes adatait tartalmazó, valamint a bankügyekkel kapcsolatos iratokat (szerződés, számlaegyenleg, stb.) ne dobja ki, tartsa őket elzárva, hogy azok ne juthassanak illetéktelenek birtokába.
- Felhívjuk figyelmét, hogy a bankok soha nem kérnek e-mailben, telefonon vagy SMS-ben ügyfél-azonosítót, belépési jelszót, PIN-kódot, bankkártya-adatokat.
- Amennyiben elektronikus banki szolgáltatást vesz igénybe, ellenőrizze a weboldal eredetiségét. A bankok és más pénzügyi intézmények valódi honlapján a böngésző alsó sávján és felső címsorában szerepel a biztonságos kapcsolat meglétét jelző lakat-ikon.
- Amennyiben egy banki oldalon a megszokottól eltérő megjelenést, furcsa nyelvezetet, vagy azonosítási kérést tapasztal, azonnal szakítsa meg az internetkapcsolatot az adott weboldallal és vegye fel a kapcsolatot a banki ügyfélszolgálattal.
- A kártékony programok ellen úgy tud védekezni, hogy az Ön által használt szoftvereket jogtiszta módon megvásárolja és szakszerűen telepíti a saját gépére.
- Mindig legyen aktív vírusirtó a számítógépen.
- Óvakodjon a kéretlen emailben, felugró ablakokban, vagy hirdetésekben kapott linkektől, mert lehet, hogy hamis vagy megtévesztő webhelyre mutatnak.
- Válasszon mindig erős jelszót, és ne használja ugyanazt minden webhelyhez.
- Rendszeresen ellenőrizze bankszámlája forgalmát, hogy azon nem történtek-e ismeretlen eredetű terhelések.