# ELBIR

Elektronikus Lakossági Bűnmegelőzési Információs Rendszer

2016. november


**A Vas Megyei Rendőr-főkapitányság Gazdaságvédelmi Alosztályának felhívása a gazdálkodó szervezetek sérelmére elkövetett internetes bűncselekmények megelőzésére**

Az elmúlt évtizedek során a számítógépek elterjedése átformálta az üzleti élet szereplőinek tervezési, termelési, értékesítési és az ezeket kiszolgáló működési folyamatait. Hasonló változás zajlott le a közszférában is. A mobil távközlési technológiák és az internet megjelenése újabb lendületet adott az átalakulásnak. Napjainkban mind a gazdálkodó szervezetek és ügyfeleik között, mind e szervezeteken belül korábban elképzelhetetlen mennyiségű információ áramlik. Az információk átadásának és feldolgozásának számos mozzanata emberi beavatkozás nélkül zajlik.

A hatékonyság fokozása iránti igény és az emberi teljesítőképesség természetes korlátainak együttes hatásaként a döntéshozatal egyre fokozódó mértékben támaszkodik automatizált folyamatokra, sőt, esetenként maga a döntés és annak végrehajtása is átkerül ebbe a körbe. Részben e tényezők állnak a szervezeten belüli munkafolyamatok és az azokhoz rendelt információ-hozzáférés szigorú behatárolása mögött is.

A gazdálkodó szervezetek felépítésében, szervezeti kultúrájában és különösen az alkalmazott technológiájukban bekövetkezett változások új típusú sebezhetőséget is magukban hordoznak, amit a bűnözők gyorsan felismernek és igyekeznek kihasználni. A fenyegetésekkel szembeni technikai, szervezési és jogalkotási intézkedések általában utólagos, követő jellegűek. Még a legfrissebb védelmi megoldások alkalmazásával sem küszöbölhető ki minden kockázat, de kellő körültekintéssel és az esetleges kárhoz mérten csekély befektetéssel kezelhető szinten tartható. A tapasztalat azt mutatja, hogy a számítástechnikai környezetben elkövetett visszaélések többsége már egyszerű óvintézkedésekkel is megelőzhető lenne.

Hírlevelünkkel a gazdálkodó szervezetek sérelmére a világháló felhasználásával elkövetett bűncselekmények megelőzéséhez kívánunk segítséget nyújtani. Bemutatjuk a visszaélések legjellemzőbb formáit, tanácsokat adunk megelőzésükre, végül útmutatással szolgálunk a bűncselekmény észlelése utáni legfontosabb teendőkről.

A hírlevélben a „számítógép” fogalmát a szó legszélesebb értelmében használjuk, hiszen a klasszikus számítógépek mellett ma már az okosóráktól a személygépkocsik szórakoztató rendszeréig számtalan eszköz foglal magába adatfeldolgozó és adattároló egységeket, amelyeken számítástechnikai programok települnek és futnak. Ennél fogva a kockázatok is jóval változatosabb módon jelennek meg, mint akár néhány évvel ezelőtt.

## A gazdálkodó szervezetek sérelmére elkövetett internetes bűncselekmények legjellemzőbb formái

### Utalásos csalás

A világhálónak köszönhetően az eladók és a vevők minden eddiginél gyorsabban találhatnak egymásra. Ugyanakkor a kínálat és a kereslet mögött álló vállalkozások adatai, sőt, részben üzleti kapcsolataik és egyedi szerződéseik is bárki számára megismerhetővé válnak. A vállalkozás honlapján referenciaként

feltüntetett üzleti partnerek kiléte, a nyilvánosságra hozott üzleti jelentések és bankszámlaszámok, a közbeszerzési folyamatok közzétett adatai, de akár egy munkavállaló óvatlansága is visszaélésre alkalmas információt adhat rossz kezekbe.

Az úgynevezett utalásos csalás során az elkövetők a megismert információmorzsákra építve ráveszik a sértettet, hogy a megvásárolni kívánt áru, vagy szolgáltatás ellenértékét az ő ellenőrzésük alatt álló bankszámlára utalja át. A bűncselekménynek két jellemző formáját különböztetjük meg.

Az egyik esetben az elkövetők a kifejezetten e célra általuk létrehozott egyedi honlapon, vagy más, törvényesen működő vállalkozás által létrehozott, üzleti hirdetésekre szakosodott honlapon árut kínálnak eladásra. Gyakran létező, jó hírű gazdasági társaság nevével visszaélve teszik ezt. A gyanútlan ügyfél maga lép kapcsolatba az elkövetőkkel a megadott elektronikus levélcímen, illetve telefonszámon. A levélcím általában vállalati címnek látszik, magába foglalja az eladóként feltüntetett társaság elnevezését, vagy annak rövidítését. Az elkövetők az áruhoz kapcsolódóan szerződést, tanúsítványt, fényképet tesznek közzé és küldenek a megrendelőnek, majd vételárelőleg és más jogcímeken – biztosítás, adminisztrációs költség – a lehető legtöbb alkalommal részösszegek átutalását kérik.

Más esetben az elkövetők beférkőznek a sértett és egy ügyfele között fennálló üzleti kapcsolatba. Ennek során manipulálják a két fél közötti kommunikációt úgy, hogy magukat – elsősorban az elektronikus levelezés során – a „másik" félnek adják ki. Közlik a vevővel, hogy az eladó bankszámlaszáma megváltozott, vagy átmenetileg nem használható, ezért újat adnak meg. Amennyiben sikerül behatolniuk valamelyik fél informatikai rendszerébe, arra is lehetőségük nyílik, hogy a megrendelés, illetve a kifizetés részleteinek egyeztetésére és valós mivoltának ellenőrzésére szolgáló üzeneteket maguk válaszolják meg a címzett helyett.

Az elkövetők az átutalt összeget készpénzben felveszik, vagy nyomban továbbutalják másik, általában külföldi bankszámlára.

**Áruvásárlási csalás**

Az elkövetők a vevő szerepét magukra öltve veszik fel a kapcsolatot a sértettel és elérik egy tételnyi áru általuk megadott címre szállítását anélkül, hogy azért fizetnének. Az eladót még nagyobb mennyiség jövőbeli, visszatérő megrendelésével kecsegtetik, aki a „jövedelmező" üzleti lehetőség bűvöletében időlegesen elfogadja az állítólagosan már átutalt ellenérték be nem érkezésére adott magyarázatokat. A cselekmény e szakaszában általában nem lepleződik le a csalárd szándék: egyrészt az esetleges visszaellenőrzés éppen az elkövetők által létrehozott kommunikációs csatornán folyik; másrészt a külső információforrások (pl. cégnyilvántartás) részben egyezést mutatnak az elkövetők által közöltekkel.

A megadott címre érkező áru gyorsan értékesítésre, illetőleg továbbszállításra kerül.

**Adatlopás**

A gazdálkodó szervezetek által kezelt személyes adatok, üzleti, bank- és adótitok, ~~és~~ valamint az egyéb titokkörbe tartozó adatvagyon önmagában is jelentős értéket képvisel. Illetéktelen kezekbe kerülésük veszélyezteti az érintett személyek érdekeit, e mellett az adatlopás, vagy az adatvesztés puszta híre is üzleti veszteséget okozhat.

Az elkövetők különböző módszereket használnak a jogosulatlan hozzáférés érdekében. Bizonyos esetekben kártevő programot, vagy kódot telepítenek a sértett számítástechnikai eszközeire, amelyek akár a billentyűzet-leütések figyelésével, vagy a jelszavak és más érzékeny adatok keresésével megszerzett

információkat továbbítják hozzájuk. Esetenként a felhasználó számára észrevétlenül átveszik az irányítást a számítógép felett, majd a fertőzött eszközt és használójának azonosító adatait további számítógépek elleni támadásokra is felhasználhatják. A megismert adatok jellegétől függően – felhasználónév, jelszó, bankkártyaadatok, elektronikus levelezési címek és telefonszámok, személyes adatok, üzleti iratok – akár átutalási és vásárlási műveleteket is végezhetnek a jogosult terhére, akár a korábban ismertetett utalásos csalást követhetnek el.

A kártevők települhetnek a számítógéphez csatlakoztatott eszközről, a felkeresett honlapokról és a beérkező üzenetekből is.

Egy másik bevett elkövetési módszer lényege, hogy létező honlap utánzásával, adathalász elektronikus levéllel, vagy egyszerűen telefonálás útján ráveszik a sértettet a fenti információk kiadására.

Ugyancsak súlyos következményekkel járhat a tárolt adatok jogosulatlan megváltoztatása, törlése, vagy hozzáférhetetlenné tétele. A rendes üzletmenet akadályozása, az ügyfelek körében bekövetkező bizalomvesztés, a dokumentumokhoz való hozzáférés blokkolásával elkövetett zsarolás közvetlenül károsíthatja a gazdálkodó szervezetet.

A fenti cselekmények alkalmasak lehetnek csalás, információs rendszer felhasználásával elkövetett csalás, információs rendszer vagy adat megsértése és más bűncselekmények gyanúja megállapítására. Az így megszerzett pénzzel végzett további műveletek pénzmosás gyanúját alapozhatják meg.

## Óvintézkedések

### Általános jellegű óvintézkedések

● A számítástechnikai eszközök és programok rendelkezhetnek biztonsági résekkel, amelyeket a fejlesztők igyekeznek felfedni és befoltozni. Ezért fontos az egyes eszközök alapfunkcióit vezérlő program (firmware), az operációs rendszer és a telepített alkalmazások naprakészen tartása, a biztonsági ***frissítések telepítése***. Egy hálózat védettségét a leggyengébb láncszem határozza meg, ezért érdemes az összekapcsolva működő számítógépek és programok paramétereinek összehangolása.

● Célszerű egyszerű vírusirtó helyett valamennyi online és offline fenyegetés elleni, az egyes eszközöket és a hálózatot is védő ***komplett biztonsági csomag*** használata. A biztonsági szoftver folyamatos futtatása és frissítése mellett ütemezett teljes rendszerellenőrzést is kell végezni. Egyetlen biztonsági szoftver sem nyújt önmagában tökéletes védelmet, ezért helyes eljárás időközönként más adatbázist használó alkalmazással is vizsgálatot végezni.

● Egy eszköz használatba vételekor a gyárilag alapértelmezett jelszót nyomban meg kell változtatni, a továbbiakban pedig rendszeresen le kell cserélni. A különböző alkalmazásokhoz ***különböző jelszavakat*** kell rendelni.

● A böngészők és egyéb programok felhasználónév-, jelszó- és űrlapadat-megjegyző funkcióit (automatikus kitöltés, ***jelszavak megjegyzése***) ki kell kapcsolni, az esetleg már mentett adatokat törölni kell.
● Az ***eszközhöz való hozzáférést***, különösen az adatbevitelt, munkaszervezési és fizikai értelemben is javasolt korlátozni:
- egy adott számítógépet egy adott felhasználó, indokolt esetben a felhasználók szűk köre kizárólagos használatában tartani;
- rejtjelező eszközt (pl. token) alkalmazni;

- a bekapcsolt, de aktuálisan nem használt számítógépet jelszavas/ujjlenyomatos billentyűzárral/képernyőzárral védeni;
- a használaton kívüli, hordozható elektronikus adathordozókat elzárni;
- a számítógépek munkavégzéshez szükségtelen csatlakozóit eltávolítani, vagy letiltani;
- a munkavállalók saját tulajdonú eszközeinek csatlakoztatását megtiltani, de legalább korlátozni és kikötni a saját eszközre telepített, naprakész biztonsági szoftver alkalmazását;
- a használaton kívüli eszközöket fizikailag is leválasztani a hálózatról;
- a feleslegessé vált adatokat törölni, a használatból véglegesen kivont adathordozókat fizikailag is megsemmisíteni.

● A ***hálózat biztonsága*** érdekében tanácsos:
- a szervert külön helyiségben elhelyezni;
- előnyben részesíteni a vezetékes hálózati csatlakozást;
- a hálózati megosztó eszközökön beállítani a MAC cím szerinti szűrést, így csak a meghatározott, egyedi azonosítóval rendelkező számítógépek csatlakozhatnak a hálózatra;
- a szervezet belső hálózatában működő berendezések számára kizárólag egyetlen, központi, tűzfallal védett átjárót biztosítani a világhálóhoz.

● A különösen fontos adatok ***biztonsági tárolására*** és az ilyen munkafolyamatok végzésére érdemes külön számítógépet, illetve hordozható tárolót alkalmazni, azt a hálózattól és – saját perifériáitól eltekintve – más eszközöktől fizikailag is elválasztani. A biztonsági mentést rendszeresen el kell végezni.

● ***Számítástechnikai felhő*** igénybe vétele hasznos az adatok biztonsági mentése céljából is, ugyanakkor fokozottan ügyelni kell a hozzáférési szabályok betartására. Vegyük figyelembe, hogy az adattárolás fizikailag külföldön történhet, ahol a harmadik személy általi hozzáférés gyakorlati és jogi lehetőségei eltérhetnek a hazai adatvédelmi szabályozástól!

● Javasolt az ***online banki műveletekhez*** kapott egyszeri biztonsági kódot más csatornán és más eszközre kérni. Bár kényelmes mindent egy eszközön, példának okáért az okostelefonunkon intézni, amennyiben ugyanazt a platformot használjuk a netbankolás műveleteire és a biztonsági kódot tartalmazó üzenet fogadására, az eszköz fertőzése esetén felesleges kockázatnak tesszük ki magunkat.

● A szervezeten kívül dolgozó személynek, valamint a szervezeten belül dolgozó, de arra kifejezett felhatalmazással nem rendelkező személynek nem szabad megadni a bankszámla, bankkártya, informatikai eszköz, vagy program használatához szükséges jelszót, számkódot, biztonsági kérdést és választ. Az erre irányuló telefonhívást, elektronikus levelet ***adathalászként*** kell kezelni.

● A számítógéphez ***távoli hozzáférést*** kérő megkeresést célszerű megtagadni. Amennyiben mégis feltétlenül szükséges, kizárólag saját informatikus felügyelete mellett, a munkahelyi vezető engedélyével és korlátozott időre történjen.

● Kerülni kell az ismeretlen és nem ellenőrizhető feladótól érkező ***kéretlen üzenetek*** és csatolmányaik megnyitását.

**Csalás és adatlopás megelőzése**

● ***Új üzleti kapcsolat létesítésekor*** egyeztessük a partner által saját honlapján, vagy egyéb úton közölt információkat az elérhető adatbázisokkal (cégnyilvántartás, az adóhatóság, a kamarák és egyéb szakmai szervezetek nyilvántartásai, stb.)!

- A magyar cégjegyzék tartalmazza a gazdasági társaság valamennyi pénzforgalmi számláját, az azokat vezető szolgáltatók nevét és székhelyét, továbbá a vezető tisztségviselők adatait és a cég elektronikus kézbesítési címét is. (A nyilvántartás adattartalma az Európai Unió egyes tagállamaiban eltérő lehet.)
- Már az interneten végzett egyszerű keresés is hasznos információkkal szolgálhat a cég nevével történt visszaélésről, vagy más, a nevében elkövetett jogsértő cselekményekről. Több honlap gyűjti és közzéteszi a bűncselekmények során használt személyneveket.
- A megadott, illetve a kapcsolattartás során kijelzett telefon- és telefaxszám tényleges előfizetője nyilvános adatbázisokból és visszahívás útján kontrollálandó. A gyanús hívásokra használt telefonszámok értékelésével több honlap is foglalkozik.
- Amennyiben a társaság elnevezésével két honlapot is találunk, a jelenség mögött meghúzódhat teljesen ártatlan ok is (pl. új honlapra történő átállás, különböző piacok igényeinek megcélzása), de okozhatja a legális honlap utánzása is.
- A cím ellenőrzéséhez az adott településhez kapcsolódó hivatalos honlapok és nyilvános térképes alkalmazások is támpontul szolgálhatnak.

● Ne csak az üzleti partner ügyintézőjével lépjünk kapcsolatba az ő közvetlen elérhetőségén, hanem a ***cég központi irodáján*** keresztül jussunk el hozzá, egyúttal megbizonyosodva arról, hogy az illető jogosult a szóban forgó üzlet megkötésére. Például felhívhatjuk a megbízható forrás révén megállapított központi telefonszámot és kérjük az adott ügylettípussal foglalkozó szervezeti elem vezetőjét.

● Óvatosságra adnak okot a tárgyalások során felbukkanó újabb és újabb, a szokásos üzletmenettől eltérő, homályos rendeltetésű, a jogi szabályozással összhangban nem álló ***költségelemek***.

● A ***már működő üzleti kapcsolatban bekövetkező változásokat*** – új bankszámla, új szállítási cím, új kapcsolattartási mód – javasolt ellenőrizni. Az üzleti partner korábbról ismert kapcsolattartójával személyesen, vagy telefonon történő egyeztetés mellett a cégnyilvántartás is számos támpontot nyújt. Az egyik kommunikációs csatornát érintő változásról (pl. e-mail-cím módosulása) indokolt másik, változatlan csatornán (pl. faxon) visszacsatolást kérni.

● Fontos a ***beérkező elektronikus levél*** küldője pontos címének ellenőrzése.
- Az elkövetők kihasználják, hogy – a levelezőrendszer beállításaitól függően – a küldő postafiókban látható neve nem feltétlenül azonos a tényleges elektronikus levelezési címével, így a címzett ismerőstől érkezettnek tekinti a küldeményt. A tényleges cím általában felfedhető úgy, hogy a kurzort a megjelent név fölé visszük, vagy megtekintjük a levél jellemzőit.

(Példa: a tényleges ügyfél postafiókban látható neve „Bízhat Bennünk Zrt.”, címe bizhat.bennunk.zrt@...hu, míg az elkövetőktől érkező levél küldőjeként ugyancsak a „Bízhat Bennünk Zrt.” olvasható, azonban a kurzort az elnevezés fölé helyezve láthatóvá válik, hogy a feladó a csalozrt@...hu.)
- Másik módszer, hogy az elkövetők a tényleges partnerétől csupán egy-két karakterrel eltérő e-mail-címet hoznak létre, a különbség azonban a napi üzleti levelezés során nem is tűnik fel. (Példa: a valós ügyfél bizhat.bennunk.zrt@...hu címéhez hasonló bizhat.bennunk.zrt.@...hu.)

● Az ***átutalás alapjául szolgáló bizonylat*** (utalásos csalásnál jellemzően pro-forma számla) adatait össze kell vetni a partnerről beszerzett és a konkrét ügylet vonatkozásában egyeztetett adatokkal. A bizonylaton látható formai elemeket – logo, aláírás, stb. – hasonlítsuk össze a korábban, illetve az egyéb forrásból megismertekkel!

● A ***partner bankszámlaszáma*** alapján ingyenes internetes adatbázisokból megállapítható a számlavezető pénzügyi intézmény, általában a számlavezető fiók is, valamint a nemzetközi bankszámlaszám (IBAN) és az intézmény területi hovatartozása (országa). Ezek eltérése a szerződésben szereplőtől gyanúra ad okot.

● Az átutalást, illetve az áru útba indítását megelőzően célszerű áttekinteni a szerződéskötés menetét és ***másik dolgozóval ellenőriztetni*** legalább a pénzügyi kondíciók egyezését.

● A fenti óvintézkedéseken túl érdemes ellenőrizni a ***szállítási cím*** létezését és annak kapcsolatát a megrendelővel.

● Fokozott körültekintéssel kell kezelni a szállítmányozás már rögzített részleteit illető ***„sürgős" módosításokat***, így a szállítási cím, szállítmányozó vállalkozás/sofőr/jármű változását.

● A teljesítésről nem csupán írásban, de a már korábbról ismert, vagy leellenőrzött kapcsolattartó révén szóban/telefonon, valamint lehetőség szerint harmadik fél – például az áru ellenértékét fogadó bank – útján is kérjünk visszaigazolást! A következő részügylet indításával célszerű várni az előző ***részügylet teljesítésének*** kétséget kizáró megerősítéséig.

● A jogszabály alapján megőrzésre kötelezett bizonylatokon túlmenően, az ügylet maradéktalan teljesüléséig tanácsos ***megőrizni*** a kapcsolódó üzleti levelezést, feljegyzéseket is.

**Ha mégis bekövetkezik …**

● Az elküldött pénzt/árut lehetőség szerint vissza kell fordítani, illetve a ***továbbküldését megakadályozni***. Az eljáró pénzügyi intézménynél haladéktalanul bejelentést kell tenni. A bank saját hatáskörében felveheti a kapcsolatot a partner pénzügyi intézménnyel, továbbá felfüggeszti az ügyleti megbízás teljesítését, ha azzal kapcsolatban pénzmosásra utaló adat, tény, vagy körülmény merül fel és annak ellenőrzéséhez a pénzügyi információs egységként működő hatóság (a Nemzeti Adó- és Vámhivatal Központi Hivatalának Pénzmosás Elleni Információs Irodája) azonnali intézkedését látja szükségesnek.

● A további részügyletek valótlannak bizonyult információk (pl. bankszámlaszám) szerinti teljesítését indokolt ***felfüggeszteni***, az üzleti kapcsolat folytatását a valós üzleti partnerrel egyeztetni.

● A ***kártevő programokat*** el kell távolítani, de legalább karanténba helyezni; a jelszavakat megváltoztatni és a fertőzött eszközöket leválasztani.

● Bűncselekmény gyanúja esetén forduljanak a területileg illetékes ***rendőri szervhez***! Bocsássák rendelkezésére az ügylettel kapcsolatos dokumentumokat és adatokat, különösen az elküldött pénz/áru sorsára, hollétére vonatkozóakat! Közöljék az érdemben nyilatkozni tudó munkatársaik, illetve üzleti partnereik nevét, elérhetőségét és szerepét!

**VAS MEGYEI RENDŐR-FŐKAPITÁNYSÁG**
**BŰNÜGYI IGAZGATÓSÁG**
**BŰNÜGYI OSZTÁLY**
**Bűnmegelőzési Alosztály**
9700 Szombathely, Petőfi S. u. 1/C.
Telefon: 06/94/ 521-065 Fax: 06/94/521-160
E-mail: bunmeg.vasmrfk@vas.police.hu