



**A Pénzügyi Szervezetek Állami Felügyelete Felügyeleti Tanácsának  
1/2009. (II.10.) számú ajánlása  
az internet-biztonsági kockázatokról**

**I.**

**Az ajánlás célja és hatálya**

Évek óta megfigyelhető az interneten keresztül nyújtott pénzügyi szolgáltatások egyre dinamikusabb térhódítása világszerte, így Magyarországon is. Ennek nyilvánvaló oka, hogy az internetes pénzügyi szolgáltatások költséghatékonyak és kényelmesek mind a szolgáltatók, mind az ügyfelek számára.

Minél több tranzakciót, nagyobb forgalmat vonz azonban magához az internetes csatorna, annál inkább csábítóvá válik a jól szervezett, technikailag képzett, multinacionális bűnözői körök számára.

A folyamattal kapcsolatban a Felügyelet felméréseket végzett, és konzultált a felügyelt intézményekkel, valamint a társhatóságokkal. A felmérésekből kiderült, hogy az interneten keresztül szolgáltatást nyújtó pénzügyi szervezetek nem elég felkészültek az internetes fenyegetésekre. Emiatt tartja szükségesnek a Pénzügyi Szervezetek Állami Felügyelete Felügyeleti Tanácsa ajánlásban megfogalmazni a témával kapcsolatos elvárásait.

A fentiekből kiindulva jelen ajánlás kiadásának célja:

- az internet-biztonsággal kapcsolatos fogalmak és követelmények egységes értelmezésének, a pénzügyi szervezetek biztonságos működéséhez szükséges tárgyi, technikai és informatikai feltételekkel összefüggő törvényi kötelezettségek teljesítésének elősegítése a piaci szereplők számára, annak érdekében, hogy az interneten keresztül zajló biztonságos ügyintézés, és ez által a pénzügyi piacok iránti bizalom ne kerüljön veszélybe,
- hozzájárulni a pénzügyi szervezetek internet-biztonsági kockázatainak tudatosításához és uralható szinten tartásához, a szektor ellen irányuló internet-biztonsági fenyegetések megelőzése, illetve szabályozott és optimális kezelése érdekében.

Az ajánlás címzettjei azok a pénzügyi szervezetek, amelyek interneten keresztül (is) igénybe vehető szolgáltatásokat nyújtanak, vagy terveznek nyújtani.

Az ajánláshoz kapcsolódó normaanyagok:

- A hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény (Hpt.) 13. § (Személyi és tárgyi feltételek) különös tekintettel a 13./B § (Az informatikai rendszerek biztonságáról),
- A magánnyugdíjról és a magán nyugdíjpénztárakról szóló 1997. évi LXXXII. törvény (Mpt.) 44. § (1) (Személyi és tárgyi feltételek)
- Az Önkéntes Kölcsönös Biztosító Pénztárakról szóló 1993. évi XCVI. törvény (Öpt.) Informatikai rendszer védelme 40./C §
- A biztosítókról és a biztosítási tevékenységről szóló 2003. évi LX. törvény (Bit.) 65. § b,

- A befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény (Bsztv.),
- 283/2001. (XII. 26.) kormányrendelet (a befektetési és az árutőzsdei szolgáltatási tevékenység, az értékpapír letéti őrzés, az értékpapír letétkezelés, valamint az elszámolóházi tevékenység végzéséhez szükséges személyi, tárgyi, technikai és biztonsági feltételekről) 7. § (Informatikai rendszer védelme)
- 2005. évi XXV. törvény a távértékesítésről

Az ajánlás a jogszabályi rendelkezéseket, a kiadott felügyeleti ajánlásokat nem ismétli meg. Amennyiben a jogszabályok az ajánláson túlmutató követelményeket írnak elő, az ezeknek való megfelelést a Felügyelet megköveteli.

Az ajánlásban a kifejezések esetenként angol nyelven (is) történő jelzése a Felügyelet azon törekvését fejezi ki, hogy az elfogadott nemzetközi terminológiák a tartalmukat lefedő lehető legpontosabban kerüljenek közvetítésre a magyarországi pénzügyi szervezetek számára.

## II.

### Preambulum

1. A törvényi kötelezettségek teljesítése, és a pénzügyi közvetítői rendszerbe vetett bizalom megőrzése érdekében a Felügyelet elvárja a pénzügyi szervezetektől az optimális internet-biztonság megteremtését.
2. Ezzel összefüggésben alapkövetelmény, hogy a pénzügyi szervezet „A Pénzügyi Szervezetek Állami Felügyeletének 1/2007. számú módszertani útmutatója a pénzügyi szervezetek informatikai rendszerének védelméről” alapján, biztonságosan működtesse informatikai rendszerét.

## III.

### A pénzügyi szervezetek internet-biztonságával kapcsolatos elvárások

3. A Felügyelet elvárja, hogy a pénzügyi szervezet rendszeres időközönként, de legalább kétfévente, végezzen az internet-biztonsági kockázatokra kiterjedő belső felmérést, amelyben meghatározza:
  - **A védelmi** biztonsági osztályba sorolást, felméri és kiválasztja azokat az objektumokat és működési folyamatokat (*informatikai rendszerek, alkalmazások, rész rendszerek, adatbázisok, adatok, üzleti folyamatok stb.*), amelyek internet-biztonsági védelméről valamilyen módon gondoskodnia szükséges.
  - A védelmi biztonsági osztályba sorolt elemek internetbiztonsági fenyegetettségét, az esetleges károk intézményre, ügyfélre gyakorolt hatásait.
  - A választott elemek és azok fenyegetettsége számszerűsített kockázatait (károk és gyakoriság). A fenyegetés–objektum párosokhoz biztonsági kockázat rendelendő elvárva a módszertan dokumentáltságát, módszertani mélység előírása nélkül. Elterjedt számszerűsítés a kárérték és a bekövetkezési gyakoriság szorzata, de pénzügyi szervezetek internet-biztonsági kockázatainak tekintetében kifinomultabb megközelítést célszerű alkalmazni.

- **A kockázat kezelését**, egyes internet-biztonsági kockázatokat elfogadhatónak vagy csökkentendőnek értékelve. A csökkenteni kívánt kockázatok esetén a kockázat-kezelés írja elő azokat az intézkedéseket, amelyek az adott kockázatot elfogadható szintre csökkentik.
- **A felmérést a pénzügyi szervezet** az évente végzendő működési kockázat felmérésbe szervesen integrálja, és figyelembe veszi a működési kockázati tökeszükséglet meghatározásánál, továbbá az eljárási szabályok/védelmi intézkedések karbantartásánál. Az internet-biztonsági kockázatok számszerűsítése egy nagyobb egység, a működési kockázatok számszerűsítését célzó intézményi eljárás részét képezi.

4. A Felügyelet javasolja, hogy a pénzügyi szervezet szabályzataiban, eljárásrendjeiben határozza meg azon tevékenységek, területek körét, amelyeket internet-biztonsági szempontból kiemelt kockázatúnak minősít, és ezért a kockázatértékelését két évnél rövidebb időszakonként kívánja elvégezni.

5. A kockázatok felmérését és kezelését követően a pénzügyi szervezet szükség szerint frissíti a biztonsági koncepcióját, amely az alábbiakat tartalmazza:

- Biztonsági stratégia: célok, alapelvek, felelősségi határok
- Jelenlegi állapot *(a kockázatelemzés eredményei)*
- Szükséges intézkedések meghatározása
- A szükséges intézkedések végrehajtási menetrendje, határidőkkel
- Az intézkedések kölcsönhatásainak analízise

6. A Felügyelet elvárja, hogy az online szolgáltatást nyújtó pénzügyi szervezetben legyenek eljárásrendek az internet-biztonsággal kapcsolatosan. Az internet-biztonsági eljárásrendek többek között szabályozzák az ügyfelekkel való állandó és rendkívüli kapcsolattartás módját és technikai feltételeit. Fontos, hogy az eljárásrendek, különösen az incidenskezelési terv, az előírt rendszerességen túl, incidens esetén, szükség szerint, soron kívül is frissüljenek.

7. Az internet-biztonsági eljárásrendekhez kapcsolódóan elvárt a nemzetközi szakirodalomban megjelenő minimum standardok és best practice eljárások, várható veszélyek és a kapcsolatos kockázati tipológia állandó követése, és ennek alapján, szükség szerint, a saját kockázati elemzések frissítése. A környezeti változások állandóan szükséges figyélésével és elemzésével párhuzamosan, a változó fenyegetéseket és kockázatokat is újra kell értékelni, hogy az indokolt változtatásokat érvényesíteni lehessen a megelőzésben, védekezésben, eljárásrendekben és a képzésben.

8. Szükséges továbbá, hogy az internet-biztonság megvalósítása, és az azzal foglalkozó szervezeti egység szervesen illeszkedjék a pénzügyi szervezet biztonsági szervezetébe, ahol azt a feladatra dedikált, képzett szakemberek képviselik, megfelelő felelősségi, döntési hatáskörrel.

9. A Felügyelet elvárja, hogy az online szolgáltatást nyújtó pénzügyi szervezetnek legyen monitorozási stratégiája az internetes üzleti tevékenységgel, és az ahhoz tartozó internet-biztonsággal kapcsolatban. A stratégia tartalmazza a szokatlan tevékenység észlelésére, és a megfelelő riasztási eljárásra vonatkozó automatizmusokat.

10. Felügyelet célszerűnek tartja, hogy az online szolgáltatást nyújtó pénzügyi szervezet internetes szolgáltatásaira vonatkozó belső szabályozásaiban és a szolgáltatás igénybevételéhez szükséges szerződéseikben az internet-biztonság kockázataival pontosan és érthetően meghatározott felelősségi elvek mentén foglalkozzon.

11. Az online szolgáltatást nyújtó pénzügyi szervezet munkatársai közül azokat, akik a szolgáltatás nyújtásában érintettek, különböző, szerepükhöz igazított képzésben és továbbképzésben javasolt részesíteni. A képzés elengedhetetlen része annak ismertetése, hogy miként lehet végrehajtani az internet-biztonsággal kapcsolatos előírásokat a napi gyakorlatban. A munkatársakat rendszeresen tájékoztatni szükséges a környezetet, a szabályzatokat és az eljárásokat érintő változásokról.

12. A képzést illetően a Felügyelet elvárja, hogy legyen részletes képzési koncepció az internet-biztonsággal kapcsolatban, külön a kiemelt szakemberek, külön az ügyintézők, és külön az ügyfelek számára. A koncepció tartalmazza:

- A célcsoportokat
- A képzési tematikákat a célcsoportok számára
- A képzéseket irányító, végző szakemberek képesítését
- A képzések időrendjét, beleértve a továbbképzéseket
- A koncepció, és egyes elemeinek életciklusát, és a szükséges frissítéseket
- A képzések hatékonyságának mérését.

13. A Felügyelet javasolja, hogy a pénzügyi szervezet rendszeresen (szükség esetén akár évente) végeztesse internet-biztonsági független, külső auditálást. Ennek alapján rögzítse a pénzügyi szervezet működési kockázatain belül az internet-biztonsággal kapcsolatos kockázatokat, hogy időben kialakítható legyen a kockázatmenedzselés.

14. Elvárt, hogy az auditálást olyan szakemberek irányítsák, akik pénzügyi szervezetek internetes üzletágában gyakorlattal, tapasztalattal rendelkeznek, annak érdekében, hogy a belső sebezhetőségek is feltárhatók legyenek. Ezen túl célszerű, hogy rendelkezzenek referenciával az internet-biztonság területén is, hogy az auditálás internet-specifikus paramétereinek kijelölését, és az eredmény elemzését megfelelő anyagismerettel legyenek képesek elvégezni.

#### **IV.**

#### **A pénzügyi szervezetek interneten keresztül nyújtott szolgáltatásaival kapcsolatos internet-biztonsági elvárások**

15. A Felügyelet elvárja a pénzügyi szervezetektől, hogy az interneten keresztül nyújtott szolgáltatásokkal kapcsolatos üzletág átláthatóan illeszkedjék a szervezeti hierarchiába, döntési, kompetencia és felelősségi viszonyai legyenek egyértelműek.

16. Az internet nyílt, globális hálózat, amely lényegét tekintve nem biztonságos. A pénzügyi szervezeteknek különböző, egyre veszélyesebb biztonsági fenyegetések kockázataira, és azok kezelésére szükséges felkészülniük. Mindezek miatt elengedhetetlen, hogy a pénzügyi szervezetek a fenyegetésekkel és a kockázatokkal arányos, erős biztonsági intézkedéseket, kontrollokat építsenek ki.

17. A pénzügyi szervezeteknek szavatolniuk szükséges az interneten bejelentkező ügyfelek azonosításának és az interneten keresztül bonyolított tranzakciók hiteles és kielégítő biztonságát. Ehhez feltétel a kontrollok megvalósítása, és egy biztonsági stratégia kidolgozása, amely maradéktalanul teljesíti az alábbi célokat:

- Adatok bizalmassága
- Rendszer sérthetlensége
- Rendszer elérhetősége
- Ügyfél és tranzakció hitelessége
- Ügyfél és ügyfél azonosítók védelme

18. A Felügyelet elvárja, hogy bizalmas adatokhoz csak megfelelő szintű jogosultsággal lehessen hozzáférni. Célszerű, hogy a pénzügyi szervezet olyan titkosítást alkalmazzon online rendszerében, amely az operációs és hálózati kockázatok alapján szükséges és elégséges.

19. Jelen ajánlás nem írja elő sem a titkosítás fajtáját, sem az erősségét, de elvárja a pénzügyi szervezetektől, hogy internetes alkalmazásaik biztonsági követelményeit rendszeresen kiértékelve olyan titkosítást használjanak, amely arányos a megkövetelt sérthetlenség és bizalmasság mértékével, és megfelel a nemzetközi szabványoknak és standardoknak.

20. Az adatvédelem általános elveivel összhangban, az ügyfél PIN kódjának és más, hasonlóan kényes adatainak biztonságát alkalmazás szinten ajánlott kezelni, elejétől a végéig (end-to-end at the application layer). Ez annak szükségességét jelenti, hogy a titkosítási folyamat sértetlen és érintetlen maradjon az adat beérkezésétől a végső rendeltetési helyéig, ahol a kítitkosítás (decryption) a titkosítás feloldása, illetve a hitelesítés zajlik.

21. A rendszer sérthetlensége az ügyfél és pénzügyi szervezet között zajló információk áramlásának, tárolásának és feldolgozásának pontosságára, megbízhatóságára és hiánytalan teljességére vonatkozik.

22. A pénzügyi szervezetek számára ajánlott olyan monitoring és megfigyelő rendszerek telepítése, amelyek jeleznek rendhagyó aktivitás, illetve szokatlan tranzakciók esetén.

23. Az online (interneten keresztül nyújtott) szolgáltatások magas szintű elérhetősége szükséges az ügyfelek bizalmának elnyeréséhez, illetve megőrzéséhez. Az összes biztonsági intézkedés hiábavaló, ha a rendszer nem elérhető, amikor az ügyfélnek szüksége van rá. A pénzügyi szervezet által nyújtott online szolgáltatásokkal kapcsolatos ügyfél elvárás a közel 24 órás rendelkezésre állás, az év minden napján, azaz szinte zéró rendszerkiesés, valamint az ehhez kapcsolódó szolgáltatási szint deklarálása és biztosítása az intézmény és az ügyfél kapcsolatában.

24. A rendszer magas szintű elérhetőségének fontos tényezői: az egyidejű felhasználói igényeknek megfelelő kapacitás (folyamatos monitorozás és szükség esetén bővítés mellett), a megbízható teljesítmény, a gyors válaszidő, a skálázhatóság és a hiba esetén a gyors helyreállítás képessége.

25. Az online szolgáltatások szempontjából a háttérrendszerek ugyanolyan fontosak, mint az internetes kapcsolatot biztosító rendszer. A rendelkezésre állás az ügyfelek kiszolgálásához a

szükséges háttérrendszerekre, és az üzletmenet folytonossági tervben rögzített, kapcsolódó háttér megoldásokra is vonatkozik (pl.: online szolgáltatást nyújtó befektetési vállalkozások szolgáltatáskiesése esetén fax igénybevétele).

26. A pénzügyi szervezetektől elvárható, hogy az üzleti célú naplózáson túl, megfelelő monitoring eszközökkel figyeljék folyamatosan a rendszer teljesítményét, a szerver folyamatokat (server processes), a forgalom mértékét, a tranzakciós időtartamokat, a kapacitás kihasználását, hogy biztosítani tudják a minimális rendelkezésre állás kiesést az online szolgáltatásoknál.

27. Az ügyfél és a tranzakció hitelessége szempontjából célszerű tekintettel lenni az alábbiakra:

- a) A pénzügyi szervezet és az ügyfél között interneten keresztül bonyolított, online kapcsolat során kétirányú adatáramlás zajlik. Amikor tranzakcióról beszélünk, mind a két fél lehet kezdeményező, illetve címzett. Ezért a tranzakció hitelessége egyformán elvárás mind a két irányban..
- b) Az adatáramlás integritása tekintetében ugyanolyan fontos például az ügyfél által indított pénz átutalási kezdeményezés információinak sérthetlensége, mint a válaszul küldött visszaigazolás hitelessége a pénzügyi szervezettől.
- c) A pénzügyi szervezet azt is vizsgálja, hogy az azonosított ügyfél által kezdeményezett tranzakcióhoz az ügyfélnek jogosultsága van-e (szerződés vagy üzletszabályzat alapján stb).

28. Az ügyfél azonosítás során a pénzügyi szervezet felelős azért, hogy megerősítse a bejelentkező személy azonosságát a pénzügyi szervezetenél nyilvántartott és meghatározott jogosultságokkal rendelkező ügyféllel. Az azonosításhoz felhasználható különböző információk közül a többfaktoros azonosítás legalább kettőt igényel:

- Amit az ügyfél tud (jelszó, PIN, egyéb saját adatok stb.)
- Amit az ügyfél birtokol (token, smart kártya, mobil telefon stb.)
- És maga az ügyfél (ujjlenyomat, arckép stb.)

29. A Felügyelet elvárja a pénzügyi szervezetektől, hogy az interneten keresztül nyújtott szolgáltatásaik során, a kockázati szintnek megfelelően az interaktív és tranzakciós kapcsolatokban mindenképpen kétfaktoros azonosítási eljárást alkalmazzanak.

30. Célszerű nagyobb értékű tranzakciók, kényes ügyféladatok megváltoztatása esetén a kétfaktoros azonosítás második szintjének ismételt megkövetelése.

31. A tranzakció tartalmi integritása annak biztosítását és ellenőrzését jelenti, hogy a tranzakciót nem módosíthatták a továbbítás során. Elvárt, hogy a hitelesített és titkosított összeköttetés teljes egészében maradjon sértetlen a kapcsolat közben. Bármilyen interferencia esetén a kapcsolatot azonnal meg kell szakítani, az érintett tranzakciókat függőben hagyva, és az ügyfelet mihamarabb értesítve valamilyen csatornán (email, telefon). A tranzakció adatai sérthetetlen módon őrzendők meg.

32. A tranzakció eredetének bizonyítására a megőrzött tranzakciós üzenet tartalmazzon olyan adatot vagy információt, ami csak a tranzakció engedélyezett kezdeményezőjétől származhat. A Felügyelet felhívja a figyelmet, hogy az eredet letagadhatatlansága önmagában még nem biztosítja a tranzakció teljes védelmét.

33. Az átvétel letagadhatatlansága védelmet nyújt a tranzakció kezdeményezőjének arra az esetre, ha a címzett rendszerében nem lenne igazolható a tranzakció. A címzett igazoló üzenetet küld vissza a kezdeményezőnek. Az üzenet tartalmazzon olyan információkat, amelyek csak az eredeti tranzakciós üzenetből származhatnak. Egyszerű sorszámozás nem elégséges. A Felügyelet által jónak tartott gyakorlat szerint, az átvételt visszaigazoló üzenetnél is gondoskodni szükséges a hitelesítésről és a tartalom integritásának ellenőrzéséről.

34. A tranzakciós üzenetek sorrendbe rendezése védelmet nyújt a címzettnek az üzenetek elvesztésével vagy megtévesztő másolásával szemben. Ez a pénzügyi szervezetek egy részénél törvényi kötelezettség is (például: online szolgáltatást nyújtó befektetési vállalkozások).

35. A pénzügyi szervezetek interneten keresztül nyújtott szolgáltatásai során az ügyfél érdekeinek és személyes adatainak védelme alapvetően fontos. Az utóbbi években rendkívüli módon elszaporodtak az olyan célzott támadások, amelyek az ügyfél személyes, azonosításra alkalmas adatainak megszerzését célozzák. Kölcsönös megegyezésen alapuló technikák segítségével az ügyfél is meggyőződhet a pénzügyi szervezet valódiságáról az online kapcsolat során. Ilyen módszer lehet például: meghatározott, megszemélyesített üzenetek, képek kiválasztása, vagy titkos kérdés-válasz előre rögzített információ alapján stb. Az ügyfél SSL kapcsolatban megvizsgálhatja a pénzügyi szervezet weboldalának tanúsítványát. A fentiekkel összefüggésben elvárt, hogy a pénzügyi szervezetek a tranzakciós ügyfél kapcsolatok során a kétfaktoros azonosítást annak szerves részeként, szükség szerint, olyan biztonsági elemekkel is egészítsék ki a folyamatban, amelyek minimalizálják a „man-in-the-middle” (man-in-the-browser, man-in-the-application) típusú támadások kockázatát.

36. Az interneten keresztül bonyolított interaktív kapcsolat pénzügyi szervezet és ügyfél között, internet-biztonság szempontjából, három helyszínre bontható

a) A pénzügyi szervezet informatikai részlegénél erre a célra kialakított alkalmazások rendszere:

- Belépési pont (többnyire az intézmény webes felülete)
- Ügyfél azonosítást és jogosultság ellenőrzést végző alkalmazások
- Ügyfél információt, kérést fogadó alkalmazás
- A válaszokat beszerző, az intézmény más rendszereivel kapcsolatot létesítő alkalmazás
- A válasz továbbítása az ügyfélhez
- A kérések és a válaszok integritásának biztosítása, ellenőrzése, titkosítása stb.
- A folyamatok monitorozását, naplózását végző alkalmazások (visszakereshetőség)

b) Az ügyfél által használt alkalmazások

- Számítógép + operációs rendszer
- Böngésző
- Biztonsági alkalmazások (vírusirtó, tűzfal, spyware figyelő stb.)
- Azonosításhoz szükséges eszköz (token, mobil telefon stb.)

c) Az internetes csatorna, amely az ügyfelet a pénzügyi intézménnyel összeköti

- Böngészőn keresztül kialakított felület
- Interaktív kapcsolat lehetősége
- Kétoldalú adatáramlás biztosítása
- Titkosított (SSL) kommunikációs csatorna

37. A Felügyelet akkor tekinti biztonságosnak az ügyfél és a pénzügyi szervezet közötti interaktív internetes kapcsolatot, ha az ügyfél azonosítása kétséget kizáró, és az interaktív online kommunikáció során az információ kétoldalú áramlása a teljes tartalmi integritás, az adatbiztonság, a folyamatos hitelesség és a visszavonhatatlanság elvének megfelel.

38. Az ügyfelet a pénzügyi szervezet ösztönzi az internetes csatorna használatára, így annak biztonságos használatáért felelős is az ügyféllel szemben. Elvárt ezért, hogy mind a pénzügyi szervezet oldali biztonságról, mind az internetes csatorna biztonságáról a pénzügyi szervezet gondoskodjon, legjobb tudása szerint (nemzetközi gyakorlat figyelembe vétele, kockázatelemzéssel megalapozott módszerek, stb.), és ismertesse az ügyféllel azokat a biztonsági elvárásokat, amelyek megvalósítását az ügyféltől elvárja.

39. Indokolatlan és aránytalan az ügyféltől olyan (akár a szolgáltatási szerződésben is rögzített) kötıtségeket kívánni a biztonság érdekében, amik számára túlzottan bonyolultak, elviselhetetlenül kényelmetlenek és/vagy túlzott anyagi áldozatot követelnek, hiszen az interneten keresztül nyújtott szolgáltatások igazi vonzereje pont az, hogy kényelmesek, egyszerűek és költséghatékonyak.

40. Rendkívül fontos ugyanakkor az ügyfelek széles körű tájékoztatása, hozzásegítése a megfelelő információkhoz és útmutatásokhoz, mert az ügyfélnek annál inkább lesz bizalma a pénzügyi szervezet online szolgáltatásaiban, és annál inkább fogja betartani az előirt biztonsági intézkedéseket, minél teljesebben megérti azokat.

### **Záró rendelkezések**

41. Az ajánlás a Pénzügyi Szervezetek Állami Felügyeletéről szóló 2007. évi CXXXV. törvény 12. § (1) bekezdés d) pontja szerint kiadott jogi eszköz, melynek rendelkezései a működő szolgáltatókon kívül a piacra lépő szolgáltatókra is kiterjednek.

42. A Felügyeleti Tanács által kiadott ajánlás tartalma kifejezi a jogszabályok által támasztott követelményeket, a Felügyelet jogalkalmazási gyakorlata alapján alkalmazni javasolt elveket, illetve módszereket, a piaci szabványokat és szokványokat. A Felügyelet ellenőrzi, hogy a pénzügyi szervezet szabályzatában foglalt rendelkezések megfelelnek-e a Felügyeleti Tanács által kiadott jelen ajánlásnak és összeveti a szolgáltatók erre vonatkozó gyakorlatát, eltérő gyakorlat esetén felhívja a szolgáltatót az ajánlásnak megfelelő szabályozás kialakítására.

## **Az interneten keresztül nyújtott pénzügyi szolgáltatások terjedése**

1. Évek óta megfigyelhető az interneten keresztül nyújtott pénzügyi szolgáltatások egyre dinamikusabb térhódítása világszerte, így Magyarországon is. Ennek nyilvánvaló oka, hogy az internetes pénzügyi szolgáltatások költséghatékonyak és kényelmesek mind a szolgáltatók, mind az ügyfelek számára. Az internet alapú szolgáltatások sikeres biztosítási, tőkepiaci, befektetési szolgáltatási és banki üzletággá váltak az elmúlt években: a GKI és a Sun Microsystem felmérése szerint 2008-ban az internetbanki szolgáltatásra szerződött ügyfelek száma megközelíti a 2 milliót (1,7 millió lakossági és 270 ezer vállalati ügyfél).
2. Minél több tranzakciót, nagyobb forgalmat vonz azonban magához az internetes csatorna, annál inkább csábítóvá válik a jól szervezett, technikailag képzett, multinacionális bűnözői körök számára. A nemzetközi pénzügyi szektorban dolgozó IT-biztonsági szakemberek 80%-a komolyan aggódik, hogy a rosszindulatú programok (malware) érzékeny üzleti adatokat lopnak tőlük (Finjan Web Security Survey 2008). Az Egyesült Királyságban például az adathalászat (phishing) által okozott közvetlen kár a 2004-es 12,2 millióval szemben 2006-ban már 33,5 millió angol font volt, miközben az elmúlt években az adathalász támadások 2.369 db/negyedévről 10.235 db/negyedéves nagyságrendre nőttek (APACS 2008).
3. Ez a nemzetközi folyamat elérte Magyarországot is.
4. A jövőben Magyarországon még dinamikusabban terjed majd az internet használat.
5. A hazai közintézmények internet ellátottsága elérte a 97%-ot (BellResearch), és így az internetes ügyintézés egyre inkább elfogadhatóvá és elfogadottá válik.
6. Az ITTK 2006-os adatai szerint a 14 és 17 év közötti magyar fiatalok 90 százaléka használja már aktívan a világhálót.
7. A magyar fiatalok szokásait, értékrendjét vizsgáló kutatás szerint a 14-17 éves korú magyar fiatalok 67 százaléka naponta, további 21 százaléka hetente többször internetezik. Tízből hét tizenéves tagja valamilyen közösségi oldalnak.
8. Ezek az adatok előrevetítik a fokozódó keresletet a pénzügyi szervezetek internetes szolgáltatásai iránt.
9. A nemzetközi elemzések jelzik, hogy a felügyelt szektorok elkötelezettsége az internetes szolgáltatások kínálata felé egyre inkább a piaci verseny által megkövetelt üzleti szükségszerűséggé válik.

10. A világban már több mint 11 millió különböző rosszindulatú program (malware) létezik, és az interneten minden 5 másodpercben 1-1 új weboldalt fertőznek meg rosszindulatú céllal (Sophos 2008. július).

11. Ebből következik, hogy a Felügyelet és a pénzügyi szervezetek egyre több, és egyre veszélyesebb internetes visszaélési kísérlettel fognak találkozni a jövőben Magyarországon is.

## A pénzügyi szervezetek által az interneten keresztül nyújtott szolgáltatások

### Az online (interneten keresztül nyújtott) szolgáltatások sajátosságai

1. Az internet nyitott és dinamikus jellegéből következik, hogy az online szolgáltatások lényegesen kockázatosabbak, mintha zárt hálózatokat, dedikált csatornákat használnánk.
2. A fokozott veszélyhelyzet miatt speciális kontrollokat és biztonsági eljárásokat kell kialakítani az online szolgáltatások kockázatainak kezelésére. A pénzügyi szervezetek különböző internetes szolgáltatásaikhoz az adott szolgáltatásnak megfelelő biztonsági szinteket és intézkedéseket rendelnek.
3. A kockázat mértéke nem független az online szolgáltatás fajtájától. Kockázati szempontból az online szolgáltatásokat három kategóriába sorolhatjuk: kizárólag információt nyújtó szolgáltatás (egyirányú, statikus), interaktív információcsere és tranzakciós szolgáltatás.

### Az online szolgáltatások típusai

#### *Kizárólag információt nyújtó szolgáltatás*

4. Az online szolgáltatások legalapvetőbb fajtája az egyirányú kommunikáció, amely információt, reklámot, akciókat stb. közvetít az ügyfél számára.
5. A kapcsolódó kockázatok sokáig nem voltak jelentősek, a közvetített információk sérülése legfeljebb reputációs kockázatot jelentett a pénzügyi szervezetnek.
6. Az új támadási stratégiák azonban, amelyek része, hogy mérgezett (poisoned) internetes oldalakon keresztül érik el a látogatók számítógépét, és úgy fertőzik meg azokat, indokoltá teszik a pénzügyi szervezetek internetes honlapjainak (webpage) fokozott, szigorú védelmét. A pénzügyi szervezetek, mint a tájékoztatásért felelős közzevők, gondoskodnak saját honlapjuk hamisíthatatlanságról, különös tekintettel arra, hogy ügyfeleik általában ezen az úton érik el az online szolgáltatásokat.

#### *Interaktív információcsere nyújtó szolgáltatás*

7. Ezek a szolgáltatások kockázatosabbak az előbbinél, tekintettel arra, hogy itt az ügyfél aktívan, kezdeményezően kommunikál az intézménnyel, kérdéseket tesz fel, igénylőlapot tölt ki, egyenleget kérdez le stb.
8. A kockázat mértéke attól függ, hogy milyen alkalmazást (application) vehet igénybe az ügyfél, illetve az általa küldött információt milyen formában és mélységben fogadja be a pénzügyi szervezet informatikai rendszere.

9. Nem elhanyagolható kockázatot jelent, hogy az ilyen jellegű szolgáltatáshoz is szükséges az ügyfél azonosítása, és az erre szolgáló rendkívül kényes ügyféladatok védelme.

*Tranzakciós lehetőséget is nyújtó szolgáltatás*

10. Ezek a szolgáltatások lehetővé teszik, hogy az ügyfél pénzügyi tranzakciókra adjon megbízást online, mint például pénz átutalás, díjfizetés, betétlekötés stb.

11. Ez a legkockázatosabb fajtája az online szolgáltatásoknak, mert az így adott pénzügyi megbízások gyorsan, automatikusan és többnyire visszavonhatatlanul teljesülnek.

12. Az egész rendszer kiszolgáltatottá válhat, ha a biztonsági kontrollok nem megfelelőek.

13. A kockázatot növeli, hogy a rendszer elleni támadás nem igényel személyes, fizikai jelenlétet, végrehajtható akár a világ másik végéből.

14. A kockázat sajátos jellemzője, hogy a támadás gyorsan, rövid idő alatt történik, valós időben többnyire észre sem vehető, és azt sem könnyű megállapítani, hogy ki, milyen módszerrel és honnan támadott.

## **A pénzügyi szervezetek interneten keresztül nyújtott szolgáltatásait veszélyeztető internet-biztonsági fenyegetések**

2007 májusában az Európai Bizottság kiadott egy kommunikét „a cyber-bűnözés elleni harc irányelveiről” (Defining the European Commission's global policy on the fight against cyber crime). Ebben megállapította, hogy a cyber-bűnözésnek (cyber crime) még elfogadott fogalmi meghatározása (definition) sincs, és javasolt egy három pontból álló definíciót:

1. Az elektronikus kommunikációs hálózatokon, információs rendszeren keresztül elkövetett hagyományos bűnözési formák, mint például a csalás és hamisítás.
2. Az elektronikus médiában terjesztett illegális tartalmak (pl.: pedofília vagy faji gyűlöletkeltésre alkalmas anyagok).
3. Az elektronikus hálózatokra specializálódott bűnözés, mint az információs rendszerek elleni támadások, DOS / DDOS és hacking (számítógépes kalózkodás).

Ugyanebben az anyagban a Bizottság nyolc problémakört határozott meg:

1. A társadalom, az üzleti élet és az állampolgárok növekvő kiszolgáltatottsága a cyber-bűnözés kockázatai miatt.
2. A cyber-bűnözők támadásainak fokozódó technikai rafináltsága és gyakorisága.
3. A következetes EU-szintű irányelvek és törvénykezés hiánya a cyber-bűnözés elleni harcban.
4. A cyber-bűnözés ellen fellépő szervek együttműködésének speciális nehézségei, amelyek részben a bűnözés határokat átlépő jellegéből adódnak, részben a nagy térbeli távolságból az elkövető és az áldozat között, és részben a kivételes gyorsaságból, amellyel ezeket a bűncselekményeket végre lehet hajtani.
5. A megfelelő szakértelem és technikai eszköztár megteremtése.
6. A közszféra és az üzleti élet döntéshozói között a hatékony együttműködési struktúra hiánya.
7. A felelősségi és kártérítési rendszer tisztázatlansága, mind az alkalmazások, mind a számítógépes szoftverek és hardverek biztonságosságának tekintetében.
8. A cyber-bűnözés kockázatai által érintett fogyasztói körben a tudatosság és a felismerés hiánya.

Az internet-biztonságot fenyegető kockázatok tekintetében új korszakba léptünk.

- Az illegálisan megszerzett személyes adatok piaca, forgalmi értékét tekintve, 2007-ben az Egyesült Államokban, versenyben volt a kábítószer piaccal és a prostitúcióval.
- A piaci lehetőségek kiaknázására létrejött több tőkeerős és technikailag jól felszerelt nemzetközi szervezett bűnözői hálózat is a multinacionális nagyvállalatok mintájára.
- A szervezeti hierarchia és a földrajzilag diverzifikált munkamegosztás tökéletesen megfelel a modern vállalatépítési elveknek, ráadásul hatékonyan fedezi a rendvédelmi szervektől az így kialakított bűnöző hálózatot.

A szervezett bűnözői hálózat megjelenése teljes egészében megváltoztatta az elkövetés módszertanát és folyamatát.

1. A munkamegosztásban az első társaság megszerzi az internetbanki jelszavakat (vagy a bankkártya adatait, PIN kóddal együtt), és értékesíti azokat az interneten anonim adatbrókereknek. Ők tovább forgalmazzák az adatokat a „pénztárosoknak” (cashiers), akik készpénzt varázsolnak az adatokból. A pénzmosásnak is saját munkamegosztása van. Lánc-email hálózatok (spammers) toborozzák a strómanokat (money mules), akik saját számlájukon fogadják a bankátutalásokat (legtöbbször naiv balekként becsapva), és felveszik készpénzben, hogy továbbküldjék egy harmadik országba, készpénzt továbbító vállalkozásokon (például a Western Union) keresztül.

2. Újabban már az internetbanki jelszavak megszerzése is munkamegosztásban történik. Adathalászok (phishermen) valódi banki oldalnak látszó weboldalakat működtetnek, ahová a lánc-email hálózatok (spammers) irányítják az ügyfeleket. Mind az adathalászok, mind a lánc-email hálózatok olyan rosszindulatú-program író csapatokat (malware writers) bérelnek, akik komplex szerszámokat, eszköztárakat (hacking tools, kits) adnak a kezükbe, amelyekkel ártatlan tulajdonosok számítógép millióit képesek kompromittálni, és saját céljaikra felhasználni (botnets).

3. Egy új szakma is létrejött, a robot-hálózat pásztor (botnet herder), aki a kompromittált számítógépek (zombie) millióit menedzseli, és adja bérbe a lánc-email hálózatoknak vagy az adathalászoknak. A robot-hálózatokat ezen kívül valódi cyber támadásokra is fel lehet használni, meg lehet zsarolni egy céget, egy üzletágot vagy akár egy egész országot az internetes forgalmának teljes megbénításával (pl.: egy online fogadóiroda, vagy a CNN, vagy Észtország). Ez a veszély a pénzügyi szervezeteket is fenyegeti.

4. A számítógépes kalózkodás (hacking) virágzó üzletág lett, és eszköztára tömegtermékként árasztja el a piacot. A bűnözésre használható rosszindulatú programok (crimeware) már semmiféle speciális tudást nem igényelnek, aki megveszi, azonnal használhatja őket, mint bármilyen más közönséges programot, a használati utasítás szerint, súgó, FAQ (Gyakran Ismételt Kérdések) és online support (webes segítség) igénybevételével. Billentyűfigyelő kémprogramok, adatlopó-továbbító programok és phishing oldal szerkesztők bérelhetők vagy vásárolhatók az interneten és egyszerű grafikai felület segítségével használhatók, ugyanúgy, mint a megszokott, közönséges kép vagy szövegszerkesztők.

5. Az így beszerezhető programok minősége egyre jobb, a fejlesztők komoly befektetéssel, valódi kutatással, fejlesztéssel, teszteléssel és ügyfélszolgálattal támogatják termékeiket. A legtöbb eszközt a vírusirtók (anti-virus szoftverek) ismeretében fejlesztik, így a mutáns rosszindulatú programokat a vírusirtók nem ismerik fel. Mire frissítik a vírusvédőket, a rosszindulatú programok már újabb változatban jelentkeznek. Egyre gyorsuló fegyverkezési verseny ez, az online támadó és védekező hadseregek között.

6. A bűnözésre használható rosszindulatú programok (crimeware) leggyakoribb terjesztési formája a trükkös email csatolmány és a fertőzött, mérgezett weboldal. A szervezett bűnözés azonban saját piaccgazdaságát is megteremti. Például, az úgynevezett „affiliate marketing program” keretében a webmestereket érdekeltté teszik abban, hogy az általuk felügyelt weboldalakra rosszindulatú programot telepítsenek. A webmesterek jutalékot kapnak (0.08-0.50 USD) minden egyes megfertőzött számítógépért, ha a rosszindulatú programot az ő oldalukról töltötte le a mit sem sejtő, ártatlan felhasználó.

7. Collective Internet Attacks (CIA, ahogy a humorral rendelkező informatikusok nevezik), az Együttes Internet Támadás, a következő lépés a fegyverkezési versenyben. Ebben az SQL injekció (SQL injection), Web-based Exploits (programhibák kihasználása), Botnet (robot-hálózat) taktikák és rosszindulatú programok (malware) felhasználásával összetüzet zúdítanak a

gyanútlan, és többnyire elővigyázatlan felhasználók számítógépeinek kompromittálására, a gépek fölötti irányítás, hatalom megkaparintására, és a piacon értékesíthető adatok megszerzésére.

8. Az első ilyen támadásnak 2008. első felében lehettünk tanúi, amikor néhány nap alatt több mint negyedmillió weboldalt mérgezték meg, köztük üzleti cégek, bevásárló központok, iskolák, média és kormányzati intézmények oldalait.

9. Ami az egészben a legijesztőbb, hogy mindebből az egyszerű felhasználó semmit sem vesz észre. Nem is sejtí, hogy a számítógépe esetleg már egy robot-hálózat része, és valaki más irányítja, kívülről (zombie).

10. A rosszindulatú programok (malware) elleni védekezés alapja az utasítás sorokból kiszűrhető és azonosítható jellegzetes kód (signature), amely olyan, mintha a program aláírása lenne. Amikor a vírusvédő program egy új vírust vagy kémprogramot talál, megkeresi ezt az aláírást (signature), és ennek birtokában a továbbiakban bármikor felismeri és szűrni tudja az újra bejelentkező rosszindulatú programot.

11. Ha azonban nem találja a program aláírását a rosszindulatú programok listájában, nem képes tilos programként felismerni a behatolót, és beengedi a számítógépre.

12. A rosszindulatú programok észlelésének elkerülésére a cyber-bűnözők összekeverik a programutasításokat (code) és teleírják értelmetlen sorokkal, összezavarva a programot azonosítani próbáló vírusvédelmet (code obfuscation). Az elrejtett aláírást nem találva, a védelem ártalmatlannak ítéli a rosszindulatú programot.

13. Ezt a technikát még tovább fejlesztették a cyber-bűnözők. A megkevert utasítás sorokat kifinomult titkosítási módszerrel teszik megfejthetetlenné. Az utasítások végrehajtásához szükséges megfejtő kulcsot pedig egy távoli szerverről kapja a rosszindulatú program az interneten keresztül.

14. A viselkedés mintán alapuló védelmi alkalmazások kimutatták, hogy a rosszindulatú programok 80%-a annyira megkevert utasítás sorokkal dolgozik, hogy azt a szokásos védelmi, illetve behatolás gátló programok nem képesek felismerni.

15. Újabb változatokban ezeket a titkosított, rosszindulatú programokat ártalmatlannak tűnő PDF és Flash fájllokba rejtik a cyber-bűnözők. Egy ilyen PDF fájl az összes vírusvédővel megvizsgáltattak, és csak 10% gyanakodott arra, hogy a fájl veszélyes.

16. Már megjelentek éles fenyegetésként, és a jövő kockázatait előrevetítve a „man-in-the-middle” típusú, célzott támadások.

A fokozódó fegyverkezési versenyben a cyber-bűnözés mindig új támadási technikákat talál. Az egyik rendkívül hatásos, régi-új módszer, az emberek természetes, bizalomra való hajlamának kihasználása, manipulálása (social engineering). Ennek segítségével maga a becsapott felhasználó ad engedélyt saját védelmi alkalmazásainak hatástalanítására, mert azt hiszi, hogy a weboldal, vagy a program, amellyel kapcsolatba került, teljesen legális, és számára érdekes, fontos. Az ilyen, emberi hiszékenységet kihasználó technikák ellen csak a felhasználók folyamatos, napra kész figyelmeztetése, tájékoztatása és rendszeres oktatása nyújthat védelmet. A fejlődés ívét tekintve, jól látszik, hogy a jövőben technikailag egyre kifinomultabb, egyre nehezebben megelőzhető és kivédhető támadásokra kell számítani.

### *A belső árulás veszélye*

A Cyber–Ark 300 rangidős (senior) IT munkatárs körében végzett felmérést, akik 1000 főnél nagyobb vállalatoknál dolgoznak. 16

- A kérdezettek fele beismerte, hogy munkájukhoz szükségtelen információkhoz is hozzáférnek adminisztratív jelszavukkal.
- Csaknem százan elismerték, hogy olyan bizalmas információkhoz is hozzáférnek, mint a bérfizetések részletei, személyes levelek (email), és ülések jegyzőkönyvei.
- Az adminisztratív jelszavak harmadát csak negyedévente cserélik, és 9 % állandó, amely még akkor is hozzáférést biztosít az alkalmazottnak, amikor már régen otthagya a céget.
- A kérdezettek fele elmondta, hogy senkitől nem kell engedélyt vagy felhatalmazást kérnie ahhoz, hogy bármilyen bizalmas információt lekérdezzon.

Az élesben üzemelő rendszert fenyegető tényezők mellett a fejlesztési folyamatban is vannak biztonsági kockázatok. Erre az esetre a legkézenfekvőbb példa, amikor egy rossz szándékú fejlesztő olyan kódot helyez el a banki rendszerben, amely sem a bank, sem az ügyfél szándékait nem tükröző működést eredményez: például az ügyfél jelszavát továbbítja egy külső e-mail címre.

**Pénzügyi szervezetek tájékoztatási kötelezettsége az általa nyújtott internetes szolgáltatásokkal kapcsolatban**

Kapcsolódó jogszabályi előírások alapján az online szolgáltatást nyújtó pénzügyi szervezetnek tájékoztatási kötelezettsége van, amely szerint:

1. Az online szolgáltatás díjait, költségeit elektronikus úton is hozzáférhetővé kell tennie ügyfelei számára.
2. Az ügyfélnek világos és teljes körű információval kell rendelkezni az online (interneten keresztül nyújtott) szolgáltatások kockázatairól, a minimális hardver és szoftver igényről mielőtt szerződik a szolgáltatásra. Az ügyfelet pontosan és érthetően tájékoztatni kell az online szolgáltatásokkal kapcsolatos speciális jogairól és kötelezettségeiről, valamint a pénzügyi szervezet jogairól és vállalt kötelezettségeiről, beleértve a rendszerhibából és internet-biztonsági sérülékenységekből adódó problémák által okozott helyzeteket.
3. Kiemelten fontos az ügyfelek megfelelő tájékoztatása akkor, ha újdonságok jelennek meg a pénzügyi szervezet internetes szolgáltatásaiban, különösen, ha ezek az azonosítással vagy más internet-biztonsági funkcióval kapcsolatosak.
4. A pénzügyi szervezetnek tudomásul kell vennie, hogy a jogi, illetve technikai nyelvezet az ügyfél számára megértési nehézségeket okozhat, ezért az információkat mindenki által érthető, köznapi nyelven is elérhetővé kell tenni.
5. Az online szolgáltatásokra vonatkozó szerződési feltételek és kondíciók a szolgáltatáson belül is könnyen elérhetően legyenek jelen, csakúgy, mint az ügyfelekre vonatkozó biztonsági és titoktartási szabályzat előírásai.
6. Informálni kell az ügyfeleket az online szolgáltatással kapcsolatos panaszkezelési és bejelentési rendszerről, szolgáltatási probléma esetén követendő eljárásról, jogorvoslati módokról, valamint az intézmény által vállalt válaszadási formákról és határidőkről.
7. Ha cyber-bűnözők ügyfelek számlájához jogosulatlanul hozzáfértek a pénzügyi szervezet kötelessége az ügyfelet mielőbb, részletesen tájékoztatni arról, ami történt, a várható következményekről, teendőkről és a kártérítési felelőségekről.

**Az ajánlásban felhasznált szakirodalom**

- ISO 27001 – 27005
- ISACA: „GENERAL CONSIDERATIONS ON THE USE OF INTERNET”
- ISACA: „IS AUDITING GUIDELINE INTERNET BANKING”
- European Payment Council: „Customer-to-bank security threat assessment”
- ENISA (European Network and Information Security Agency) „Methods for the identification of Emerging and Future Risks”
- PTK – CERT-Hungary (2007): „A pénzüzeteket érintő internetes fenyegetések”
- MTA-SZTAKI: „Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai”
- FFIEC (Federal Financial Institutions Examination Council): „E-Banking”
- FFIEC (Federal Financial Institutions Examination Council): „Authentication in an Internet Banking Environment”
- COMMISSION OF THE EUROPEAN COMMUNITIES: „Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 EU Action Plan”
- Basel Committee on Banking Supervision 2003: “Risk Management Principles for Electronic Banking”
- FATF 2008: “MONEY LAUNDERING & TERRORIST FINANCING VULNERABILITIES OF COMMERCIAL WEBSITES AND INTERNET PAYMENT SYSTEMS”
- ENISA (European Network and Information Security Agency) „Security Economics and The Internal Market”
- Michel J.G. van Eeten and Johannes M. Bauer: „ECONOMICS OF MALWARE: SECURITY DECISIONS, INCENTIVES AND EXTERNALITIES”
- CRAMM: CCTA Risk Analysis and Management Method
- Finjan: Web Security Survey 2008
- Cisco: Internet Malware Trends 2008