A Magyar Nemzeti Bank 15/2015. számú ajánlása
az interneten keresztül nyújtott pénzügyi szolgáltatások biztonságáról

Az interneten keresztül nyújtott pénzügyi szolgáltatások biztonsága

I. Az ajánlás célja és hatálya

Az ajánlás célja az interneten keresztül nyújtott pénzügyi szolgáltatások biztonságával kapcsolatban a Magyar Nemzeti Bank (a továbbiakban: MNB) elvárásainak megfogalmazása, és ezzel a jogalkalmazás kiszámíthatóságának növelése, a vonatkozó jogszabályok egységes alkalmazásának elősegítése.

Az ajánlás alapja az MNB az internetbanki szolgáltatások biztonságáról szóló 2/2015 számú ajánlása, és kidolgozása során figyelembe vételre kerültek az Európai Bankfelügyeleti Hatóságnak (European Banking Authority, EBA) a 2014. december 19-ei, az internetes fizetések biztonságáról szóló iránymutatása[1].

Az MNB jelen ajánlás közzétételével biztosítja az Európai Bankfelügyeleti Hatóságnak az internetes fizetések biztonságáról szóló iránymutatásának való megfelelést.

Az ajánlás nemzetközi ajánlásokon és bevált gyakorlatokon alapul, ennek megfelelően a felépítése is tagolásra került: a javaslatok határozzák meg a nemzetközi ajánlásokban foglalt, az internetes rendszerek megfelelő biztonságának kialakításához szükséges feltételeket, míg az előremutató gyakorlatok bemutatják az elvárások teljesítésével kapcsolatos legjobb gyakorlatokat. Az előremutató gyakorlatok mindegyikének egyidejű kialakítása sok esetben nem lehetséges, mivel akár egymás kompenzáló kontrolljaiként is értelmezhetők. Ugyanakkor az elvárások más megoldásokkal is teljesíthetők, feltéve, hogy az adott intézkedés adekvát védelmet nyújt.

Az ajánlás – az internetes fenyegetettségek kettős irányultsága miatt – két részből áll: egyrészt az intézmények interneten keresztül nyújtott szolgáltatásaival kapcsolatba hozható belső irányítási és üzemeltetési szabályokkal, másrészt pedig az internet felől elérhető alkalmazások fejlesztési és belső biztonsági elemeivel foglalkozik.

Az ajánlás címzettjei azon, az MNB-ről szóló 2013. évi CXXXIX. törvény 39. § hatálya alá tartozó intézmények, amelyek internet alapú kiszolgálást nyújtanak ügyfeleiknek. Az MNB javasolja továbbá, hogy az elfogadó tevékenységet is folytató intézmények az önálló fizetési alkalmazást

---

1https://www.eba.europa.eu/documents/10180/1004450/EBA_2015_HU+Guidelines+on+Internet+Payments.pdf/313bf770-f673-4edf-a686-260f68422686

üzemeltető internetes kereskedőiktől és fizetésszolgáltatás integrátoroktól[2] is követeljék meg minimum elvárásként a dokumentum szerinti biztonsági intézkedések teljesítését.

Jelen ajánlásban **interneten keresztül nyújtott pénzügyi szolgáltatás (továbbiakban internetes szolgáltatás)**

a) az interneten keresztül indított, és ügyfelek számláival kapcsolatos szolgáltatások nyújtása, összefoglalóan az internetbanki szolgáltatás nyújtása,

b) a pénzforgalom lebonyolításáról szóló 18/2009. (VIII. 6.) MNB rendelet szerint a csoportos beszedési megbízás és felhatalmazó levélen alapuló beszedési megbízás teljesítésére szóló elektronikus felhatalmazás (továbbiakban elektronikus felhatalmazás) adása és módosítása,

c) az elektronikus kereskedelmi tevékenységhez (e-commerce) kapcsolódóan az interneten keresztül fizetésre alkalmas kártyával (továbbiakban fizetési kártya) – ideértve az olyan kártyaalapú fizetési megoldásokkal lebonyolított fizetést is, amelyhez egy internetes vásárlás céljára használható alternatív, ideiglenes kártyaszám tartozik, amely csökkentett érvényességi idővel, korlátozottan használható, és előre meghatározott költési limittel rendelkezik (továbbiakban virtuális kártya),

d) a kártyás fizetési adatok olyan szolgáltatás használata céljára történő regisztrálása, amely lehetővé teszi az ügyfél számára egy vagy több fizetés kezdeményezésére alkalmas eszköz adatainak a regisztrálását annak érdekében, hogy több internetes kereskedő felé hajtson végre fizetéseket (továbbiakban elektronikus tárca-szolgáltatások)

e) a személyes adatok, a bank-, biztosítási, fizetési és értékpapír titok körbe eső adatok – például ügyfél-elszámolások, számlakivonatok – ügyfelek felé internetes felületen történő közzététele,

f) a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvényben meghatározott elektronikus pénz (továbbiakban elektronikus pénz) interneten keresztül történő két elektronikus pénz nyilvántartására szolgáló számla (továbbiakban elektronikuspénz számla) közötti utalása.

Az ajánlás a fizetési kártyákhoz kapcsolódó fizetések – ideértve az elektronikustárca-szolgáltatáson keresztüli virtuális fizetési kártyákat is – lebonyolításának a biztonságával nem foglalkozik. Erre a vezető kártyatársaságok által kiadott – és ***PCI DSS*** néven ismert – *Payment Card Industry Data Security Standard* informatikai biztonsági követelményrendszer előírásai érvényesek. A PCI DSS megfelelőséget a fizetési kártya fizetési folyamatban részt vevő pénzügyi

[2] jelen ajánlásban a fizetésszolgáltatás integrátorok: a kedvezményezett (vagyis az internetes kereskedő) részére egy szabványosított kapcsolódási felületet biztosítanak a pénzforgalmi szolgáltatók által nyújtott fizetéskezdeményezési szolgáltatásokhoz.

intézmények, szolgáltatók és kereskedők számára a kártyatársaságok előírják és ellenőrzik, de az MNB is javasolja a pénzügyi intézmények számára a megfelelőség folyamatos fenntartását.

Az ajánlás hatálya az intézmények **internet felől elérhető informatikai rendszereire** és az intézmények **internet oldali hálózati környezetének** valamennyi rendszerelemére kiterjed. **Internet oldali hálózati környezet** alatt azokat az adathálózati szegmenseket kell érteni, amelyekben az internetes szolgáltatások tranzakciós adatai megjelennek.

Az internetes szolgáltatásoknak az alkalmazott kommunikációs közegtől és az ügyféloldali eszköz jellegétől függetlenül kell biztonságosnak lenniük. Ezért az ajánlás ezeket nem különbözteti meg, és egyaránt vonatkozik személyi számítógépekről, valamint hordozható (mobil) eszközökről – pl. mobilszolgáltatók hálózatát használó okos telefonokról vagy PDA-król – kezdeményezett internetes szolgáltatások biztonságára.

Az ajánlás minimum elvárásokat határoz meg, és ahol ezek valamilyen eredményre utalnak, ott az eredményt különböző egyéb eszközökkel is el lehet érni. A kifejezések esetenként angol nyelven is történő jelzése az MNB azon törekvését fejezi ki, hogy az elfogadott nemzetközi terminológia a lehető legpontosabban kerüljön közvetítésre az intézmények számára.

II.

AZ INTERNETES SZOLGÁLTATÁSOK IRÁNYÍTÁSI KÖRNYEZETE

1. Felsővezetői felügyelet

1.1. Az intézményeknek megbízható vállalatirányítási rendszerrel és megfelelő belső ellenőrzési mechanizmusokkal kell rendelkezniük. Azonosítaniuk kell az internet használatával szükségszerűen együtt járó kockázatokat, ki kell dolgozniuk és alkalmazniuk kell a saját védelmi intézkedéseiket informatikai és biztonsági fejlesztések, eszközök és szabályozások formájában. Folyamatosan követniük kell a várható támadási formákat és a lehetséges sérülékenységeket, hiszen az újabb és újabb fenyegetések újabb és újabb kockázatokat jelentenek a rendszerek működtetésére. A visszaélések megelőzéséhez, a technológiai biztonság megteremtésén túl kiemelten fontos szerepe van a felsővezetői irányításnak. Ez kiterjed a feladat- és felelősségi körök egyértelmű meghatározására, a védelmi intézkedések összehangolására és ellenőrzésére, valamint az internetes szolgáltatással kapcsolatos elvárások és intézkedések ügyfelek irányában történő közvetítésére, valamint az ügyfelek biztonság tudatosságának az erősítésére.

1.2. Az MNB javasolja, hogy az intézmény felsővezetése alakítsa ki belső irányítási rendszerét vezetői elkötelezettség, folyamatba épített ellenőrzések, beszámoltatási-, valamint független ellenőrzési eljárások formájában. Biztosítsa, hogy az intézményen belül valamennyi szakterület ismerje a saját felelősségét az internetes szolgáltatásokkal kapcsolatosan, kezelje a kockázatokat,

valamint megtegye azokat a szükséges intézkedéseket, amelyekkel a felfedezett visszaélések elkövetői ellen hatékonyan fel lehet lépni.

1.3. Előremutató gyakorlat

A felsővezetés a felelősségi körében jóváhagyja az intézmény internetes szolgáltatásra vonatkozó informatikai biztonsági szabályzati rendszerét, és gondoskodik arról, hogy az intézmény:

a) a technológiai kockázatok magas szintjéhez igazodóan folyamatosan figyelemmel kíséri az internetes fenyegetéseket, és incidenseket követően, új fenyegetések megjelenésekor, az infrastruktúra változásait megelőzően, valamint **legalább évente egyszer** átvizsgálja az internetes pénzügyi szolgáltatások nyújtásához alkalmazott informatikai rendszerét (a továbbiakban: **internetes informatikai rendszer)**, feltárja, dokumentálja a működésben rejlő informatikai kockázatokat, és gondoskodik a feltárt kockázatok kezeléséről,

b) az internetes informatikai rendszer által alkalmazott ügyfél azonosításnál, valamint a tranzakciós adatok interneten keresztül történő átvitelénél alkalmazott védelmi- és hitelesítési eljárások megfelelőségének igazolására rendelkezik az eljárások technikai szintű és áttekinthető műszaki leírásaival, melyek alapján azok működése megismerhető és szakmailag értékelhető, auditálható,

c) csalásfelderítő „fraud monitoring” rendszert működtet az internetes szolgáltatások használatában előforduló visszaélések visszaszorítására,

d) az internetes szolgáltatás rendelkezésre állásának biztosítására rendelkezik az előre nem tervezett rendszerkiesések kezelésére vonatkozóan, a feladatokat és a felelősöket is tartalmazó, az operatív tevékenységeket forgatókönyvszerűen előíró üzletmenet-folytonossági és katasztrófa-elhárítási tervekkel, és ezek megfelelőségét sikeres tesztekkel igazolja,

e) nyilvántartást vezet az internetes szolgáltatással kapcsolatos biztonsági incidensekről és ügyfélpanaszokról, és elvégzi azok rendszeres kiértékelését valamint az internetes informatikai rendszer szükség szerinti korrekcióját.

2. Az ügyféloldal biztonság

2.1. Az internetes szolgáltatások folyamatában az ügyfél magatartása, végfelhasználói eszközei jelentős kockázatot hordoznak. Az ügyfélkockázat az intézményt is fenyegetheti, azonban számos külső forrásból érkező fenyegetést az ügyfél és az intézmény együttműködésével hatékonyan ki lehet védeni. Ennek eszköze lehet az ismeretterjesztés, az ügyfél-tájékoztatás, illetve az ügyféloktatás.

Az ügyfél-tájékoztatás, -oktatás, történhet például az intézmény honlapján vagy hírlevelekben nyújtott információkon keresztül, ezek tartalmukkal az ügyfelek biztonságos internet-használati ismereteit bővíthetik.

Online vásárlások esetében a fizetéshez kapcsolódó visszaélések észlelését, megakadályozását jelentősen segíteni lehet, ha az alkalmazások az ügyfél számára jól megkülönböztethetően elkülönítik a fizetési folyamatot a vásárlás egyéb folyamataitól.

2.2. Az MNB javasolja, hogy az intézmény ügyfelei részére pénzügyi szolgáltatást az interneten keresztül csak akkor tegyen elérhetővé, ha azt az ügyfél kifejezetten kéri. A szolgáltatás igénybevételét megelőzően adjon az ügyfél felé részletes tájékoztatást az internetes szolgáltatás konkrét részleteiről, valamint az ügyféloldali biztonság megteremtésére nyújtson hatékony ügyfél-tájékoztatási, oktatási tevékenységet a biztonságos internet-használati ismeretek bővítésére.

2.3. Az MNB javasolja, hogy az intézmény biztosítson legalább egy biztonságos csatornát az ügyfelekkel folytatott kommunikációra, és a biztonságos csatornán keresztül tájékoztassa az ügyfelet az internetes szolgáltatás változásairól, valamint a biztonságos csatornát használja figyelemfelhívásra a tudomására jutott kockázatok – például adathalászat vagy egyéb pszichológiai ügyfél-manipulációra vonatkozó kísérletek – esetén.

2.4. Előremutató gyakorlat

a) az intézmény az ügyféloldali biztonság kialakítása érdekében tájékoztatást nyújt az ügyfelek felé a szolgáltatás használatáról, és kitér az alábbiakra:
    i. az internetes szolgáltatás használatához az ügyfél oldalon használt berendezésre, szoftverre vagy egyéb eszközökre vonatkozó követelmények,
    ii. a tranzakciók ügyfél általi kezdeményezésére és jóváhagyására és/vagy a tájékoztatáskérésre szolgáló eljárások ismertetése, az egyes lépések következményeit is ismertetve,
    iii. amennyiben az intézmény hardver és/vagy szoftver eszközt bocsájt az ügyfél rendelkezésére, azok helyes és biztonságos használatára vonatkozó útmutatás,
    iv. a hitelesítő adatok vagy a bejelentkezéshez illetve a tranzakciók végrehajtásához szükséges hardver elemek (pl. tokenek) vagy szoftverek elvesztése vagy ellopása esetén követendő eljárás,
    v. az intézmény és az ügyfél az internetes szolgáltatás használatával kapcsolatos köztelezettségeinek és felelősségeinek az ismertetése.

b) az ügyfél oldali biztonság kialakítása érdekében az intézmény, tájékoztatást nyújt az ügyfelek felé a biztonságos internet használati ismereteik bővítésére. A tájékoztatás kitér legalább az alábbiakra:
    i. a személyi azonosítók – különösen a jelszavak és a kriptográfiai magánkulcsok – használata, biztonságos kezelése,
    ii. a kártékony kódok elleni védelmi rendszer – minimálisan vírusvédelmi rendszer – használatának jelentősége az ügyfél számítógépén,

iii. az intézmény internetes oldala valódiságának ellenőrzésével az illetéktelen támadási kísérleteket kiszűrése – SSL kapcsolatok kiépülésének ellenőrzése, URL ellenőrzése, tanúsítványhiba értékelése stb. –, az ellenőrzések elvégzésének fontossága,

iv. az internetről letöltött szoftverek kockázatai,

v. az e-mail használatának kockázata az üzenet bizalmasságára,

vi. megtévesztő tartalmú – pl. adathalász – e-mailek kiszűrése,

vii. visszaélés észlelése vagy gyanúja esetén követendő bejelentési eljárás, az ügyfélszolgálat igénybevételének a módja, és a lehetséges további teendők ismertetése,

viii. az internetes szolgáltatásoknak idegen gépről történő, valamint a nyilvános internet pontokon[3] keresztüli igénybevételének a veszélyeire, kockázataira való figyelem felhívása.

c) Az intézmény biztosítja az ügyfél bejelentések és a biztonsági kérdések folyamatos – 0-24 órás – ügyfélszolgálati fogadását, megválaszolását, valamint biztonsági intézkedések szakszerű és azonnali megtételének lehetőségét.

d) Amennyiben az intézmény biztonsági okokból adott műveletet vagy fizetés kezdeményezésére alkalmas eszköz (továbbiakban fizetési eszköz) letilt, a tiltást a biztonsági probléma lehető legrövidebb időn belüli megoldásáig tartja fenn,

e) a lehetséges kockázatok értékelése alapján a támadásokkal szembeni védelem érdekében[4] az intézmény mérlegeli, és döntése alapján az ügyfél részére biztonsági eszközöket (például megfelelő védelemmel ellátott eszközöket és/vagy egyedi kialakítású böngészőket) biztosít,

f) az elfogadó tevékenységet is folytató pénzügyi intézmény az internetes kereskedőitől megköveteli, hogy az online vásárlási munkamenetben egyértelműen elkülönítsék a fizetéshez kapcsolódó folyamatot a vásárlás folyamatától (ennek lehetséges módja például a fizetési folyamat számára új képernyő ablak megnyitása),

g) az elfogadó tevékenységet is folytató pénzügyi intézmény felvilágosító programokat szervezz a csalásfelderítés és megelőzés témakörében a velük szerződésben álló internetes kereskedők számára.

3. Tranzakciók figyelemmel kísérése

3.1. Az MNB javasolja, hogy az internetes szolgáltatás védelme érdekében az intézmény a hamis tranzakciók megelőzésére, észlelésére és letiltására csalásfelderítő („fraud monitoring”) rendszert

[3] pl. wifi pontok, internet kávézók

[4] például a böngészőbe közbeékelődő, ún. „man in the browser” típusú támadások ellen

működtessen, amely a gyanús vagy magas kockázatú tranzakciókat egyedi átvilágítási és ellenőrzési eljárásnak veti alá.

3.2. Az MNB javasolja, hogy a csalásfelderítő rendszer méretét, összetettségét és rugalmasságát az intézmény úgy határozza meg, hogy az összhangban áll a kockázatfelmérés eredményével, és az adatvédelmi jogszabályoknak is megfelel.

3.3. Előremutató gyakorlat

a) az intézmény a tranzakciókat a jóváhagyást megelőzően a csalások felderítésére alkalmas rendszerrel átvizsgálja. A felderítés alapjai lehetnek:
   i. paraméterezett szabályok - például a nyilvánosságra került vagy lopott kártyaadatok feketelistája,
   ii. az ügyfelek szokásostól eltérő viselkedésmintái,
   iii. az ügyfelek által használt belépési eszközök rendellenes viselkedésmintái (például a szokásostól eltérő IP-cím használata, ez az IP-cím szerinti földrajzi hely ellenőrzésével meghatározható[5], vagy az IP-címnek az internetes munkamenet során történő megváltozása),
   iv. az ügyfélre jellemzőtől eltérő internetes kereskedői kategóriák, vagy
   v. a szokásostól jelentősen eltérő tranzakciós adatok.

b) Az intézmény olyan rendszert alkalmaz, amely alkalmas
   i. az internetes munkamenet során bekövetkező, rosszindulatú szoftverek által okozott fertőzések észlelésére (például, ha a felhasználó helyett egy script végzi a hitelesítést), és
   ii. alkalmas az ismert csalási esetformák felismerésére.

c) A kockázatkezelési szabályzata alapján gyanúsnak vagy nagy kockázatúnak minősülő tranzakciók esetén az intézmény figyelmeztetheti ügyfeleit például telefonhívás vagy SMS útján,

d) az intézmény lehetővé teszi, hogy ügyfelei általános érvényű, személyre szabott szabályokat tudjanak megadni online viselkedésük, illetve szokásaik alapján. Ilyenek például, hogy az ügyfelek megadhatják, hogy fizetéseiket csak bizonyos, előre meghatározott országokból fogják kezdeményezni, vagy bizonyos kedvezményezetteket ún. fehér- vagy feketelistára tehetnek,

e) az intézmény a tranzakciók átvilágítását és kiértékelését a lehető legrövidebb időn belül elvégzi,

[5] A geoIP cím ellenőrzés a kibocsátó ország és a felhasználó IP-címe közötti megfelelés ellenőrzésére szolgál.

f) az elfogadó tevékenységet is folytató pénzügyi intézmény figyelemmel kíséri az internetes kereskedői tevékenységét, és a kereskedői oldalon elkövetett visszaélések észlelésére és megelőzésére csalásfelderítő rendszert működtet.

4. Az internetes informatikai rendszer belső hozzáférés-védelme, naplózása és a számon kérhetőség

4.1. Az informatikai rendszerek belső hozzáférés-védelmének alapfeladata a felhasználók azonosításával az illetéktelen felhasználók kizárása valamint a rendszerszintű jogosultsági beállításokon keresztül a felhasználók részére a rendszer-erőforrásokhoz való hozzáférések biztosítása. A felhasználók azonosításához és a jogosultságkezeléshez szükséges információk nyilvántartása a pénzügyi rendszerek biztonságos működésének egyik meghatározó pontja. A biztonságos rendszerüzemeltetéshez utólagos ellenőrzés céljából szükséges a rendszerműködés, a rendszereseményekről nyilvántartása, és a nyilvántartások megőrzése.

4.2. Az MNB javasolja, hogy az intézmény korlátozza az internetes informatikai rendszeréhez való dolgozói hozzáféréseket az üzletileg szükséges legalacsonyabb szintre, valósítsa meg a felhasználói azonosítók kezelésének és a jogosultsági beállításoknak a dokumentált és felügyelt adminisztrációját, valamint rendszernaplók vezetésével biztosítsa az informatikai rendszer korábbi állapotaira vonatkozó szakértői vizsgálatok elvégezhetőségét.

4.3. Előremutató gyakorlat

a) az internetes informatikai rendszeren belül az erőforrásokhoz való felhasználói hozzáférések korlátozva vannak azok számára, akiknek arra a napi munkájuk elvégzéséhez szükségük van, és a hozzáférési jogosultságok a munkavégzéshez szükséges legalacsonyabb szintre vannak beállítva,

b) az internetes informatikai rendszer egyes elemeinek hozzáférési jogosultsági beállításai biztosítják az internetes szolgáltatás zártságát, azaz a felhasználók csak az alkalmazást használva férhetnek hozzá az informatikai rendszer adataihoz, és a beállításokat az intézmény dokumentálja és rendszeresen ellenőrizi,

c) az intézmény a külső partnerek által végzett tevékenységeket minden esetben – akár lokálisan, akár távolról történnek – felügyelet alatt tartja, és a végzett tevékenységeket az informatikai rendszer naplózza annak érdekében, hogy azok tartalma később visszamenőlegesen is megállapítható legyen,

d) a távoli adatkapcsolatok esetileg, és csak a szükségességük idejére vannak felépítve, és a tevékenység befejeződése után azonnal bontásra kerülnek,

e) az intézmény az internet felől a tartományi eléréshez legalább kétfaktoros hitelesítést alkalmaz,

f) a felhasználói jelszavak hálózati átvitele valamint tárolása rejtjelezetten történik,

g) az internetes informatikai rendszer felhasználói jelszavainak – ideértve a kiemelt jogosultsággal rendelkező adminisztrátori jelszavakat is – kezelése az alábbiak szerint történik:

   i. a kezdeti jelszavak egyediek, és kényszerítik a felhasználót az első bejelentkezéskor annak a megváltoztatására,

   ii. a 30 napja inaktív felhasználói azonosítók a rendszerben letiltásra kerülnek,

   iii. a felhasználói jelszavak megváltoztatása legalább 90 naponként kikényszerített,

   iv. a választható jelszavak a legutolsó 5 jelszótól különböznek,

   v. a jelszavak hosszúsága legalább 8 karakter,

   vi. a jelszavak tartalmaznak kis- és nagybetűket és számokat is,

   vii. legalább 5 sikertelen belépési kísérlet után a felhasználói azonosító tiltásra kerül, és a kitiltás ideje legalább 5 perc vagy a rendszergazda újbóli engedélyezéséig tart.

h) a technikai felhasználói azonosítók – pl. alkalmazások adatbázis felhasználói – jelszavainak kezelése biztonságos, azok legalább 8 karakter hosszúságúak, legalább 90 naponként megváltoztatásra kerülnek, és a hozzáférés védelmükre – pl. jelszómegosztással – teljesül a „négy szem elve”,

i) abban az esetben, amikor egy technikai felhasználói azonosító jelszavának a megváltoztatása működési kockázatot jelent, az intézmény legalább 12 karakter hosszúságú jelszót használ, és törekszik arra, hogy minél előbb lehetővé váljon a jelszó 180 naponként történő rendszeres megváltoztatása,

j) az internetes szolgáltatás ügyfél által végrehajtott munkameneteinek tranzakciós folyamata naplózásra kerül,

k) az internetes hálózati környezet komponenseire – felhasználói azonosítókkal és idővel azonosítottan – automatikus rendszeraudit naplózás működik, legalább az alábbi tartalommal:

   i. a kiemelt – privilegizált, pl. a root vagy adminisztrátori – felhasználók tevékenységei,

   ii. érvénytelen belépési kísérletek,

   iii. sikertelen authorizációk eseményei (elutasított hozzáférési kísérletek),

   iv. audit naplók újraindítása – inicializálása,

   v. releváns rendszer objektumok létrehozása és törlése.

l) a napló állományok védettek az illetéktelen módosítások ellen, ennek érdekében:

   i. a naplóállományokért felelős rendszeradminisztrátorok valamint az internetes informatikai rendszer üzemeltetését végző rendszeradminisztrátorok kölcsönösen ki vannak zárva egymás rendszereiből vagy

ii. a napló bejegyzések utólagosan módosíthatatlan formában vagy tartós adathordozóra folyamatosan rögzítésre kerülnek.

m) napi gyakorisággal készülnek mentések a naplóállományokról, és azok az informatikai rendszer üzemi – éles – környezetétől tűzbiztos módon és hozzáférés szempontjából is elkülönítetten, fizikai biztonságát tekintve is védett és ellenőrzött környezetben megőrzésre kerülnek,

n) az intézmény rendelkezik eszközzel a napló bejegyzések tartalmi illetve logikai szűréseken alapuló vizsgálatához,

o) az intézmény biztosítja a napló állományoknak a vonatkozó jogszabályokban előírt ideig, de legalább 5 évig történő visszakereshetőségét,

p) az internetes informatikai rendszer minden egyes komponensének belső órája hiteles időszerverhez van – közvetlenül vagy közvetve – szinkronizálva.

5. Üzemeltetési biztonság

5.1. Az MNB a nemzetközi ajánlásokkal összhangban az internetes informatikai rendszerek üzemeltetésében magas informatikai biztonsági szint megvalósítását javasolja az intézmények számára. A magas biztonsági szint megteremtése a szokásos informatikai biztonsági intézkedések magas biztonsági szinten történő megvalósítását, illetve azokon felül további védelmi intézkedések bevezetését és működtetését igényli.

Ezeket a – többlet- – intézkedéseket a bevezető részben is meghatározottan az **internetes hálózati környezet** rendszer elemeire – hálózati elemek, szerverek, alkalmazások – kell alkalmazni. Hálózati elemek például a tűzfalak, routerek, switch-ek. Szerverek többek között a web-, alkalmazás-, adatbázis-, proxy-, idő-, DNS-szerverek. Alkalmazás pedig valamennyi alkalmazás, akár saját fejlesztésű vagy vásárolt, függetlenül annak technológiájától, belső vagy külső elérhetőségétől. Az **internetes hálózati környezet** alatt pedig azon hálózati szegmensek összességét tekintjük, amelyekben az internetes szolgáltatás tranzakciós adatai megjelennek.

A többlet intézkedések alkalmazása miatt az internetes hálózati környezetet célszerű olyan kisméretűre kialakítani, amilyenre csak lehet. Ez megtehető, ha az internetes hálózatokat az intézmény elválasztja egyéb hálózataitól. Az elválasztás módszere a hálózati szegmentálás, ami hálózati hozzáférési ellenőrzési listával rendelkező és a hozzáférések naplózására alkalmas eszközökkel, például belső hálózati tűzfalakkal, routerekkel megvalósítható.

5.2. Az adathálózat biztonsága

5.2.1. Az MNB javasolja, hogy az intézmény az internetes informatikai rendszerének védelmére alakítson ki biztonságos internetes hálózati környezetet.

5.2.2. Előremutató gyakorlat

a) az internetes hálózati környezet dokumentációja mindenkor aktuális, valamennyi adatkapcsolatot – ideértve a vezeték nélküli adatkapcsolatokat is – feltünteti, valamint tartalmazza a tűzfalak és a router eszközök dokumentált és jóváhagyott beállítási szabály elveit (policy),

b) az internetes hálózati környezet internet felől elérhető eszközei – pl. a kommunikációs szerverei és website-jai – DMZ-ben, az internetes szolgáltatáshoz tartozó web szervizek és a pénzügyi alkalmazások, adatbázisok a DMZ mögötti belső hálózatokon kerülnek elhelyezésre,

c) a beállításokon keresztül az intézmény biztosítja, hogy csak indokolt és jóváhagyott tűzfal szabályok működnek, és a szabályrendszerek alapértelmezetten mindent tiltanak (deny all),

d) megtörténik a tűzfal szabályok legalább 6 havonta történő felülvizsgálata és annak dokumentálása,

e) megtörténik a hálózati eszközök konfigurációs fájljainak a mentése azok minden változtatását követően,

f) az intézmény eljárást működtet a hálózati konfiguráció és a beállítások megváltoztatásának dokumentált jóváhagyására, tesztelésére és végrehajtására,

g) amennyiben vezeték nélküli hálózatok kapcsolódnak az internetes hálózati környezethez, azok tűzfal szabályrendszerekkel védve érik el a hálózati környezetet, biztonságos kriptográfiai protokollokat használnak[6], továbbá csak az üzletileg indokolt adatkapcsolatok engedélyezettek, a többi szolgáltatás tiltott,

h) az internetes hálózati környezet határvédelme során mindenhol legalább DPI (deep pocket inspection) technológia működik,

i) az intézménynél az internetes hálózati környezetére DoS/DDoS támadások elleni védelem működik.

5.3. Biztonsági paraméter beállítások

5.3.1. Az MNB javasolja, hogy az intézmény a hálózatra csatlakoztatást megelőzően változtassa meg az alapértelmezett jelszavakat és az alapértelmezett biztonsági paraméter beállításokat, valamint gondoskodjon arról, hogy az eszközök beállításai biztonságos rendszerhasználatot eredményezzenek.

5.3.2. Előremutató gyakorlat

a) az üzembe helyezésüket követően megtörténik az internetes informatikai rendszer alapértelmezett jelszavainak és biztonsági paraméterei alapértelmezett beállításainak a megváltoztatása,

[6] pl. WPA2

b) valamennyi rendszerkomponens esetében az intézmény rendelkezik biztonsági házirenddel – biztonsági beállítási szabályzattal –, amely megfelel valamely elfogadott iparági „hardening” ajánlásnak[7] és a szabályzatokat rendszeresen frissíti,

c) valamennyi rendszerkomponens esetében rendszeresen megtörténik a biztonsági házirendek alapján a beállítások felülvizsgálata, valamint a nem biztonságos illetve szükségtelen szolgáltatások – pl. szkriptek, driver-ek, portok, szervizek – törlése,

d) a nem konzolról történő rendszeradminisztrátori kapcsolatok kriptográfiai rejtjelezéssel védettek.

5.4. Biztonságos rendszerek és alkalmazások használata

5.4.1. Az MNB javasolja, hogy az intézmény biztosítsa az internetes informatikai rendszer védelmét és biztonságos működését.

5.4.2. Előremutató gyakorlat

a) az internetes informatikai rendszer elemein kártékony kód elleni védelmi rendszerek működnek. Ezek naprakész állapotúak, futnak és naplóznak. A beállításokon keresztül biztosított a rendszeres automatikus frissítés, valamint teljes vírus ellenőrzések (on demand scan) rendszeres időszakonként – de legalább heti egy alkalommal – történő elvégzése,

b) valamennyi rendszer komponensre és szoftverre előzetes tesztelések elvégzését követően, de legfeljebb 60 napon belül telepítésre kerülnek a tesztek alapján elfogadott gyártói javító csomagok,

c) a rendszerkomponensek változtatásaira, új eszközök rendszerbe állítására teljes körű változáskezelési eljárás működik, a változtatásokat és a jóváhagyásokat az intézmény dokumentálja,

d) a rendszer komponensek tesztelése úgy történik – pl. önálló, az üzemi környezettől elkülönített teszt környezet használatával –, hogy a tesztelés az üzemi működést nem veszélyezteti,

e) az internetről elérhető web alkalmazások védelmére az intézmény minden változtatást követően, de legalább évente egy alkalommal kézi- vagy automatikus eszközzel sérülékenység vizsgálatot végez[8] és gondoskodik arról, hogy a feltárt sérülékenységek javításra kerüljenek, vagy folyamatosan frissített web-alkalmazás tűzfalat (web application firewall) üzemeltet.

5.5. Biztonsági felügyeletek

5.5.1. Az MNB javasolja, hogy az intézmény felügyeleti rendszert alkalmazva, valamint az internetes informatikai rendszer audit naplóin keresztül folyamatosan ellenőrizze az internetes

[7] pl. SANS, NIST, CIS stb.

[8] web alkalmazás sérülékenység vizsgálat - web application vulnerability test

pénzügyi szolgáltatás megfelelőségét, valamint alkalmazzon technológiai megoldásokat az illetéktelen külső behatolások észlelésére és a támadások közvetlen elhárítására.

5.5.2. Előremutató gyakorlat

Az intézmény

a) a magas kockázati besorolású események észlelése esetén valós idejű riasztást alkalmaz, valamint biztosítja a védelmi intézkedések haladéktalan megtételének a lehetőségét,

b) elvégzi az audit naplók napi ellenőrzését – ideértve a biztonsági rendszerek pl. IDS/IPS vagy AAA rendszerek (pl. RADIUS szerver) audit naplóit is,

c) legalább 6 havonta wifi eszköz felderítést végez vagy vezeték nélküli behatolás felderítő eszközt (Wireless Intrusion Detection System) alkalmaz,

d) változtatások után, de legalább negyedévente elvégzi az internetes informatikai rendszer külső, és évente a belső sérülékenység vizsgálatát (external/internal network vulnerability scan),

e) változtatások után, de legalább évente elvégzi az internetes informatikai rendszer törési vizsgálatát (penetration test),

f) az internetes hálózati környezet adatforgalmának ellenőrzésére behatolás-figyelő rendszert (Intrusion Detection System, IDS) és behatolás megakadályozó rendszert (Intrusion Prevention System, IPS) alkalmaz.

5.6. Incidenskezelés

5.6.1. Az MNB javasolja, hogy az intézmény készüljön fel a munkatársai, valamint az ügyfelek által jelzett biztonsági események – biztonsági incidensek – kezelésére, ehhez dolgozzon ki hatékony incidenskezelési eljárást, az eljárást dokumentálja és annak megfelelőségét sikeres tesztek elvégzésével igazolja.

Az elfogadó tevékenységet is folytató pénzügyi intézmények kötelezzék az önálló fizetési alkalmazást üzemeltető internetes kereskedőiket arra, hogy biztonsági incidenseiket minden esetben haladéktalanul jelezzék feléjük, és működjenek együtt mind velük, mind a bűnüldöző szervekkel az események kivizsgálásában. Amennyiben az intézmény tudomására jut, hogy az internetes kereskedő nem tesz eleget együttműködési kötelezettségének, tegyen lépéseket a kötelezettség betartatása érdekében, illetve ha szükséges, bontson vele szerződést.

5.6.2. Előremutató gyakorlat

Az intézmény

a) rendelkezik az internetes szolgáltatásával kapcsolatosan dokumentált incidenskezelési eljárással, amely tartalmazza legalább az alábbiakat:

    i. szerepek, feladatok, kommunikációs és kapcsolat felvételi eljárások a hatóságokkal és felügyeleti szervekkel egy vélt vagy valós támadás, sérülés esetében,

ii. részletes gyakorlati eljárások a kártékony kód elleni védelmi- és a felügyeleti rendszerek – pl. az IDS, IPS rendszerek – riasztásainak kezelésére,

iii. részletes gyakorlati eljárások a (D)DoS támadások kezelésére,

iv. tesztelési eljárások az incidenskezelés megfelelőségének ellenőrzésére.

b) legalább évente elvégzi és dokumentálja incidenskezelési eljárásainak megfelelőségi vizsgálatát.

5.7. Szolgáltatók igénybevétele

5.7.1. Annak érdekében, hogy azok ne jelentsenek szükségtelen kockázatot, az MNB javasolja, hogy az intézmény az internetes pénzügyi szolgáltatásához igénybe venni kívánt szolgáltatók kiválasztását, valamint az együttműködés feltételeinek a kialakítását a szolgáltatás kockázatainak a mértékéhez illeszkedően, kiemelt gondossággal végezze[9].

5.7.2. Előremutató gyakorlat

a) az intézmény a szolgáltató kiválasztását megelőzően meggyőződik arról, hogy a szolgáltató informatikai biztonsági szintje a tevékenységet illetően megfelel legalább az intézményekre vonatkozó előírásoknak, illetve nem alacsonyabb a saját biztonsági szintjénél,

b) az intézmény az internetes szolgáltatás területén igénybe vett szolgáltatókkal megkötött szerződéseiben a szolgáltatásra vonatkozóan:

i. egyértelműen meghatározza a szolgáltatási szinteket, a teljesítés mérésére vonatkozó eljárásait, valamint a szolgáltató nem szerződésszerű teljesítésének eseteire vonatkozó feltételeket,

ii. egyértelműen és részletesen meghatározza a szolgáltató információbiztonsági felelősségét,

iii. kiköti az intézmény helyszíni, illetve helyszínen kívüli ellenőrzési jogát, ami kiterjed a szolgáltató alvállalkozóira is,

iv. rögzíti, hogy alvállalkozót a szolgáltató csak az intézmény jóváhagyásával alkalmazhat,

v. rögzíti a szolgáltató és esetleges alvállalkozói felelősségét a tevékenység megfelelő színvonalon történő végzéséért, valamint az intézmény azonnali felmondási lehetőségét a szerződés ismételt vagy súlyos megszegése esetére.

c) az intézmény felügyeli a szolgáltatások szerződésszerű teljesítését.

---

[9] Amennyiben az intézmény kiszervezési szolgáltatást vesz igénybe, az feleljen meg teljes körűen az intézményre vonatkozó ágazati jogszabályban a kiszervezett tevékenységre vonatkozó előírásoknak is (például a hitelintézetekről és pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény 68. §, a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény 79. §, a biztosítókról és a biztosítási tevékenységről szóló 2003. évi LX. törvény 76-78. §, stb.).

6. Üzletmenet-folytonosság biztosítása

6.1. Az ügyfélbizalom, valamint az ügyfélkiszolgálás színvonalának fenntartása érdekében az MNB javasolja, hogy az intézmény alkalmazzon olyan műszaki-technológiai megoldásokat, amelyek biztosítják az internetes pénzügyi szolgáltatás magas rendelkezésre állását. Rendelkezzen azokkal a tartalék eszközökkel illetve megoldásokkal, amelyek a nem várt kiesések eseteire biztosítani tudják az internetes szolgáltatásoknak – az intézmény által elvárt helyreállítási időn[10] belüli – újraindíthatóságát.

6.2. Előremutató gyakorlat

a) az intézmény adathálózata redundáns, „single point of failure" rendszer elemek csak a hálózati végpontokon fordulnak elő, és ezek az eszközök magas üzembiztonságúak,

b) az internetes szolgáltatás kiesésének lehetséges eseteire vonatkozóan az intézmény a szolgáltatás indítását megelőzően meghatározza azokat az – üzletileg még elfogadható – helyreállítási időket, amelyeken belül a szolgáltatás újra indulását elvárja, és ezeket az időket az informatikai rendszerben bekövetkező változások esetén minden esetben felülvizsgálja,

c) az intézmény rendelkezik azokkal a tartalék eszközökkel vagy tartalékolási megoldásokkal, amelyekkel az elvárt helyreállítási időn belül az internetes szolgáltatás működése helyreállítható,

d) az intézmény felkészült az internetes szolgáltatás kiesésére, ehhez kidolgozta az egyes kiesési esetek kezelésére vonatkozó – felelősöket és a konkrét tevékenységeket is tartalmazó – üzletmenet-folytonossági és katasztrófa-elhárítási terveit, ezeket dokumentálta és ezek végrehajtására a személyzetét kiképezte,

e) gyakorlati tesztek sikeres elvégzésével az intézmény igazolta, hogy az internetes szolgáltatást az elvárt helyreállítási időkön belül újra tudja indítani.

III.

AZ INTERNETES INFORMATIKAI ALKALMAZÁSOK

7. Az ügyféladatok védelme

7.1. Az MNB javasolja, hogy az internetes informatikai alkalmazások tervezése során az intézmény törekedjen arra, hogy a lehető legkevesebb adatot gyűjtse, valamint az adatok kezelését úgy valósítsa meg, hogy a lehető legkevesebb esetben legyen szükség az adatok tárolására, továbbítására, megjelenítésére és archiválására. Az intézmény gondoskodjon arról,

[10] elvárt helyreállítási idő: Recovery Time Objective (RTO)

hogy az adatok kezelése során – például az adatok szeparálásával vagy maszkolásával – minden lehetséges esetben vonja ki az adatokat a bank-, biztosítási, fizetési, valamint értékpapír titkot tartalmazó adatok köréből.

Az internetes szolgáltatásokat az internetes felületen biztonságos és megbízható környezetben kell elérhetővé tenni. Amennyiben az intézmény az ügyfelek felé nem biztonságos csatornán – például e-mail, SMS – kíván bank-, biztosítási, értékpapír, illetve fizetési titkot tartalmazó ügyféladatot – például elektronikus számlakivonatot – átadni, az állományt az átadás előtt tegye rejtjelezéssel olvashatatlanná.

8. Az ügyfél hitelesítése

8.1. Az internetes szolgáltatások meghatározó kockázati pontja az ügyfél személyazonosságának távoli – az interneten keresztül történő – meghatározása. Az internetes kapcsolat kezdeményezőjének hitelesítése többféle módon és többféle biztonsági szinten történhet.

Az egyfaktoros hitelesítés – felhasználói azonosító plusz statikus jelszó – internetes pénzügyi szolgáltatásokhoz nem ad megfelelő biztonságot, magas a kockázati szintje, ezért használata esetén szolgáltatási korlátozásokat kell alkalmazni.

A két- vagy többfaktoros, ún. erős ügyfél-hitelesítés a tudásnak, tulajdonnak és egyedi jellemzőnek minősíthető, alábbi elemek közül legalább kettő használatán alapul:

a) valami, amit csak a felhasználó tud, például statikus jelszó, kód, személyi azonosító szám,

b) valami, amit csak a felhasználó birtokol, például token, intelligens kártya, mobiltelefon,

c) valami, ami a felhasználó maga, például egy biometriai jellemző, mint például az ujjlenyomat.

A kiválasztott elemeknek egymástól függetlennek kell lenniük, azaz az egyik elemmel való visszaélés nem veszélyeztetheti a másikat (illetve a többit).

PKI technológia alkalmazása megfelelő biztonságot jelent, ha a kriptográfiai algoritmusok megfelelnek az ismert és szakmailag elfogadott biztonságos kriptográfiai algoritmusoknak, valamint ha az ügyfél kriptográfiai magánkulcsa biztonságos hozzáférés védelemmel ellátott aláírás-létrehozó eszközön (eToken-en, pl. kriptográfiai hardver kulcson vagy kriptográfiai (PKI) chipkártyán) kerül létrehozásra. Ebben az esetben az aláírás-létrehozó eszközön tárolt tanúsítvány – a hozzá tartozó magánkulccsal – magas biztonsági szintet jelent az ügyfél hitelesítésére.

A személyazonosítókkal kapcsolatos visszaélési esetek (identity theft) megakadályozására illetve gyors felfedésére az intézmények az internetes szolgáltatást kiegészíthetik egyéb biztonsági szolgáltatásokkal is, pl.:

a) sikeres és/vagy sikertelen bejelentkezésről, tranzakciókról SMS/email üzenetet küldhetnek a felhasználók számára,

b) virtuális billentyűzetet használhatnak az azonosítók bevitelére,

c) ismételt sikertelen bejelentkezési kísérleteket követő sikeres bejelentkezéskor captcha[11]-t alkalmazhatnak.

Az intézmény egy időben többféle hitelesítési módszert is használhat annak függvényében, hogy az ügyfél milyen műveleteket – és milyen tranzakciós limitekkel – hajthat végre az interneten keresztül.

8.2. Az MNB javasolja, hogy az intézmény internetes informatikai rendszere az ügyfélkapcsolat létesítéséhez végezzen ügyfél hitelesítést. Ennek során az alkalmazott hitelesítési módszer biztonságossága legyen arányos az interneten keresztül nyújtott pénzügyi műveletek kockázataival. Pénzügyi kötelezettséget jelentő műveletekhez PKI technológia alkalmazása – és ennek részeként biztonságos hozzáférés védelemmel rendelkező aláírás-létrehozó eszköz használata – javasolt, de ennek hiányában is legalább kétfaktoros erős hitelesítési eljárás alkalmazása szükséges.

Amennyiben az intézmény tisztán tanácsadói szolgáltatásokat nyújt, melyekben nem érintettek ügyfél- és fizetési adatok – pl. fizetési kártya adatok –, az intézmény a kockázatfelmérése alapján megfelelőnek értékelt saját hitelesítési követelményeit alkalmazhatja.

8.3. Az elektronikus kereskedelemre vonatkozó speciális ajánlások

a) A fizetési kártya kibocsátó pénzügyi intézményeknek biztosítaniuk kell a kártyabirtokos erős hitelesítésének a lehetőségét, valamint minden kibocsátott fizetőkártyának technikailag alkalmasnak kell lennie az erős hitelesítéssel való használatra.

b) Az elfogadó tevékenységet is folytató pénzügyi intézményeknek lehetővé kell tenniük, hogy a kibocsátók a kártyabirtokos erős hitelesítését elvégezhessék.

c) Az elfogadó tevékenységet is folytató pénzügyi intézmények megkövetelik a saját fizető alkalmazást használó internetes kereskedőiktől, hogy fizető alkalmazásaik tegyék lehetővé, hogy a kibocsátók a kártyabirtokosok erős hitelesítését elvégezhessék.

d) Az interneten keresztül végrehajtott fizetések esetén erős ügyfél-hitelesítést kell alkalmazni. Alacsonyabb biztonságú hitelesítési eljárás előre meghatározott alacsony kockázati kategóriába eső tranzakciók esetében alkalmazható, ilyenek például a tranzakció alapú kockázatfelmérés alapján alacsony kockázatúnak minősített műveletek, vagy a kis értékű fizetési tranzakciók[12].

---

[11] captcha: grafikus képként megjelenített, és így az internetes robotok által nem olvasható szövegrész ügyféltől való karakteres visszakérése (Completely Automated Public Turing test to tell Computers and Humans Apart)

[12] kis értékű fizetési tranzakciók: amelyek egyedileg nem haladják meg a kilencezer forintot, vagy összesítve a napi negyvenötezer forintot, továbbá azok a fizetések, amelyek a mindenkori, negyvenötezer forintot meg nem haladó rendelkezésre álló összeg terhére kerülnek teljesítésre (lásd PSD 34. cikk (1) és 53. cikk (1), valamint Pft. 2§. 16.)

e) Az elektronikus tárca szolgáltatásokat is nyújtó intézmények a szolgáltatás keretében elfogadott kártyás fizetési rendszerekre vonatkozóan írják elő, hogy a kártyakibocsátó erős ügyfél- hitelesítést végezzen, amikor a jogos birtokos első alkalommal regisztrálja a kártyaadatokat.

f) Az elektronikus tárca szolgáltatásokat is nyújtó intézmények alkalmazzanak erős ügyfél-hitelesítést, amikor az ügyfél bejelentkezik az elektronikus tárca fizetési szolgáltatásba, vagy kártyatranzakciót hajt végre az interneten. Alacsonyabb biztonságú ügyfél-hitelesítési eljárás előre meghatározott alacsony kockázati kategóriába eső tranzakciók esetében alkalmazható, ilyenek például a tranzakció alapú kockázatfelmérés alapján alacsony kockázatúnak minősített műveletek, vagy a kis értékű fizetési tranzakciók.

g) Az interneten kibocsátott virtuális kártyák adatainak generálását erős ügyfél-hitelesítés mellett kell elvégezni. A virtuális kártyák esetében az első regisztráció biztonságos és megbízható környezetben történjen, ahol az intézmény hitelessége, valamint az adatok védelme egyaránt biztosított. Ilyenek például az intézmény felelősségi körébe tartozó alábbi környezetek:

   i. az intézmény helyiségei,

   ii. az internetes banki műveletek végzésére szolgáló vagy egyéb biztonságos weboldal,

   iii. a bankautomata (ATM) szolgáltatások

h) Az intézmény és az internetes kereskedők között a fizetés kezdeményezés és a fizetési adatokhoz való hozzáférés során biztosítani kell a kétoldalú hitelesítést.

i) A fizetési kártyák kibocsátásakor ösztönözni kell a kártyabirtokosokat az erős ügyfél-hitelesítés igénylésére, illetve aktiválására.

j) Az internetes vásárlás során meg kell adni a lehetőséget az ügyfélnek, hogy – amennyiben még nem rendelkezik erős ügyfél-hitelesítéssel –, a fizetést megelőzően, az internetes kereskedő oldaláról indítva azt megigényelhesse, aktiválhassa. Ebben az esetben ezt az ügyfél biztonságos és megbízható környezetbe történő irányításával kell elvégezni.

8.4. Előremutató gyakorlat

a) az intézmény az internetes tranzakciókra vonatkozóan értékhatárokat határoz meg (például az egyes fizetések maximális összege vagy egy bizonyos időtartamon belüli összesített összeg), és lehetőséget biztosít az ügyfeleknek az értékhatárok további csökkentésére.

b) az intézmény lehetővé teszi az ügyfelek számára az internetes szolgáltatás letiltását,

c) az internetes informatikai rendszer olyan ügyfél hitelesítési eljárást alkalmaz, amelynek biztonságossága arányos a munkamenetben végezhető pénzügyi műveletek kockázataival,

d) az erős ügyfél-hitelesítés során a felhasználói azonosító mellett a statikus jelszó kiegészítésre vagy helyettesítésre kerül legalább egy, a felhasználói azonosítótól és a statikus jelszótól független azonosító adattal. A független azonosító adat lehet például:

   i. az ügyfélhez az internetes kapcsolatától biztonsági szempontból elkülönülő (out of band) másik kommunikációs csatornán (pl. SMS-ben) eljuttatott, egyszeri, véletlenszerű és időkorlátos azonosító adat – a dinamikus jelszó,

   ii. PIN kóddal vagy jelszóval védett kód előállító eszköz – pl. hardver token – által előállított időkorlátos véletlenszerű számsorozat egy eleme – a dinamikus kód,

   iii. TAN kód (transaction authentication number), az ügyfélnek korábban kiadott, egyszeri alkalommal használható azonosító kódok halmaza,

   iv. az ügyfél személyazonosságának telefonon keresztül történő hitelesítése,

   v. az ügyfél valamely biometrikus jellemzője.

e) az internetes pénzügyi szolgáltatás igénybevételéhez vagy az adatok módosításához (beleértve a fehér listák készítését és módosítását is) erős ügyfél-hitelesítés szükséges. Alacsonyabb biztonságú ügyfél-hitelesítési eljárást az intézmény az alábbi esetekben alkalmaz:

   i. az ügyfél korábban létrehozott fehér listáin szereplő megbízható kedvezményezettek felé irányuló kimenő tranzakciók,

   ii. ugyanazon ügyfél ugyanannál az intézménynél vezetett két számlája közötti tranzakciók,

   iii. ugyanazon az intézményen belüli átutalások, amelyeket a tranzakció alapú kockázatfelmérés megengedhetőnek tart,

   iv. kis összegű fizetési tranzakciók.

f) amennyiben egy intézmény kizárólag olyan tanácsadói szolgáltatásokat nyújt, amelyekben ügyfél- és fizetési adatok nem érintettek, saját kockázatfelmérése alapján alakítja ki hitelesítési eljárását. Az ügyfélkapcsolat kezdeményezésekor biztonságos kommunikációs csatornát épít ki, és az ügyfél azonosítást ezen keresztül végzi, és a biztonságos csatornát a munkamenet végéig fenntartja (pl. SSL/TLS, IPSEC),

g) a pénzügyi intézmény szervertanúsítványának érvényességi láncában szerepel az ismert böngészőkben is telepített valamelyik tanúsítvány-kiadó,

h) az ügyfelek tanúsítványa és a hozzá tartozó kriptográfiai magánkulcsa biztonságos hozzáférés védelemmel ellátott aláírás-létrehozó eszközön (eTOKEN-en) kerül létrehozásra és az ügyfelek felé kiadásra,

i) statikus jelszavak használata esetén az intézmény (legalább) az alábbi védelmi intézkedéseket alkalmazza:

i. sikertelen belépési kísérletet követően az ügyfél felhasználói azonosítójának az automatikus kitiltása legalább 10 másodpercre,

ii. legfeljebb 15 sikertelen belépési kísérletet követően az ügyfél felhasználói azonosítójának a kitiltása, és az ügyfél kérésére, biztonságos eljárással történő újbóli aktiválása,

iii. maximális időtartam beállítása, amely túllépése esetén automatikusan megszakad az internetes fizetési szolgáltatás inaktív munkamenete,

iv. sikertelen belépési kísérletekre vonatkozó figyelem felhívás küldése az ügyfél felé legkésőbb a következő sikeres belépéskor.

j) hitelesítő adatok – pl. ügyféljelszó, a független csatornán eljuttatott dinamikus jelszó illetve kód -, az alkalmazási oldalon csak az operatív memóriában, és csak a vele történő műveletvégzés idejére kerül tárolásra, ismételt felhasználáshoz azt az internetes rendszer az ügyféltől ismételten bekéri,

k) a független csatornán eljuttatott dinamikus jelszó élettartama nem több mint 10 perc,

l) a dinamikus kód élettartama nem több mint 1 perc,

m) az ügyfél azonosító adatok pénzügyi intézmény általi kezelése felügyelet és ellenőrzés alatt tartott, és kizárja az egyszemélyi visszaélés lehetőségét,

n) az ügyfél előzetes kérése alapján az intézmény azonnali értesítéseket küld számára az általa megjelölt számlái egyenlege, valamint személyi azonosító adatai változásakor,

o) amennyiben az intézmény SMS vagy e-mail, értesítést küld az ügyfél internetes számlája egyenlege, valamint személyi azonosító adatai változásakor, az adatok maszkolásával biztosítja, hogy az értesítést csak az ügyfél tudja számlához kapcsolni, az ügyfél személye az adatokból nem azonosítható, azaz az értesítés bank- biztosítási- fizetési- valamint értékpapír titkot, ügyfél- illetve személyes adatot nem tartalmaz,

p) amennyiben az intézmény bank- biztosítási- fizetési- valamint értékpapír titkot tartalmazó ügyfél adatot nem biztonságos csatornán, például SMS vagy e-mail értesítés formájában továbbít az ügyfél felé, a továbbítást megelőzően az értesítést rejtjelezéssel olvashatatlanná teszi, és az ügyfél számára a küldést megelőzően biztosítja az értesítés elolvasásához szükséges alkalmazást valamint rejtjel kulcsot (jelszót),

q) az intézmény valós idejű lehetőséget biztosít az ügyfeleknek arra, hogy a tranzakciók végrehajtási státuszát és a számlaegyenlegeket bármikor ellenőrizhessék,

r) Az internetes szolgáltatás igénybevételéhez szükséges hitelesítési eszközök, ügyfelek általi igénylése és az eszközök átadása biztonságosan történik.

9. A tranzakciós üzenetek végponti védelme

9.1. Az internetes szolgáltatások során a biztonságos csatorna (pl. SSL/TLS, IPSEC) használata mellett biztosítani kell az interneten keresztüli tranzakciós üzenetek védelmét az ügyfél számítógépe, valamint a pénzügyi intézmények web-szervizei mint üzenetvégpontok között is (end-to-end, vagy message security). A végponti védelem során biztosítani kell az alábbi négy biztonsági tényező teljesülését:

a) a bizalmasságot, azaz a tranzakciós üzenetek lehallgatás elleni védelmét,

b) a sértetlenséget, azaz tranzakciós üzenetek módosítások elleni védelmét,

c) a hitelességet, azaz a tranzakciós üzenetek küldőjének hitelesítését, valamint

d) a letagadhatatlanságot, azaz az üzenetküldés tényének a kétség kívüli bizonyíthatóságát.

Ezek teljesítéséhez az ügyféloldalon elektronikus aláírás használata javasolt. Az elektronikus aláírás az ügyfél kriptográfiai magánkulcsával hozható létre, de létrehozható – a kulcs bizalmasságát és integritását biztosító védett módon létrehozott – eseti aláíró kulcs alkalmazásával is.

Az intézménynek a letöltésre kiadott beépülő kriptográfiai modulok sértetlenségének és hitelességének az ellenőrizhetőségét is biztosítania kell.

9.2. Az MNB javasolja, hogy az intézmény internetes informatikai rendszere valósítsa meg az interneten keresztül továbbított pénzügyi tranzakciós üzenetek végponti védelmét, ennek során biztosítsa a tranzakciós üzenetek bizalmasságát, sértetlenségét és hitelességét, valamint biztosítsa az üzenetküldés letagadhatatlanságát.

9.3. Előremutató gyakorlat

a) az intézmény az internetes tranzakciók bizalmasságát és integritását kriptográfiai eljárással biztosítja,

b) az intézmény az üzenetküldő hitelesítésére az ügyfél birtokában már meglévő, vagy neki az interneten keresztül felépített munkamenettől elkülönült biztonságos (out-of-band) csatornán eljuttatott egyedi véletlenszerű azonosítót (pl. kriptográfiai magánkulcs vagy TAN kód, illetve dinamikus kód vagy dinamikus jelszó) rendel az üzenethez,

c) az intézmény a tranzakciós üzenetek sértetlenségének a megállapítására az üzeneteket elektronikus aláírással vagy kriptográfiai ellenőrző összeggel (cryptographic checksum) látja el,

d) az intézmény az üzenetküldés letagadhatatlanságát a tranzakciós üzenetek ügyfél oldali elektronikus aláírásával és időbélyeggel biztosítja, vagy az üzenetek adott pillanatban való meglétét érkezéskor illetve kiküldéskor szerver oldali elektronikus aláírással és időbélyeggel igazolja,

e) amennyiben vannak letöltődő kliens szoftverek, beépülő modulok (java appletek, active-x modulok), azok az intézmény által elektronikusan alá vannak írva.

10. Az elektronikus tranzakciók adatainak megőrzése

10.1. Az interneten keresztül nyújtott pénzügyi műveletek bizonylatai – a papír alapú megbízások hiányában – az elektronikus tranzakciók adatai. Szükséges, hogy az intézmény az elektronikus tranzakciók adatait a forgalmazásuk időpontjával együtt hitelesen megőrizze. A hiteles tranzakció állomány alapján tudja az intézmény később vizsgálni – és adott esetben bizonyítani –, hogy egy banki tranzakció forrása internet felől beérkezett elektronikus tranzakció volt-e.
Az elektronikus tranzakciók adatainak megőrzése elvégezhető többféle biztonsági szinten. A legegyszerűbb, de alacsony biztonságot nyújtó megoldás a tranzakciós üzenet és az idő összerendelése és együttes eltárolása rendszer állományokban (fájlokban). Mivel ebben az eljárásban az adatok sértetlenségének ellenőrizhetősége önmagában nem adott, a megoldás hitelessége – egyben bizonyító ereje – a rendszer állományok módosíthatóságától, illetve a módosítások elleni védettségétől, és annak hiteles biztosításától függ.
A tranzakciók hitelességének az igazolhatóságára az internetes informatikai rendszer az elektronikus tranzakciókat elektronikus aláírással és időbélyeggel látja el. Az időbélyeget az intézmény saját maga, vagy külső – esetleg minősített – időbélyegzés-szolgáltató készítheti.

10.2. Az MNB javasolja, hogy az intézmény hitelesítse az elektronikus tranzakciós üzeneteit, gondoskodjon azok biztonságos őrzéséről, valamint biztosítsa a jogszabályokban előírt ideig, de legalább 5 évig azok visszakereshetőségét és hitelességük igazolhatóságát.

10.3. Előremutató gyakorlat

a) az intézmény az internetes pénzügyi szolgáltatás tranzakciós üzeneteit elektronikus aláírással és időbélyeggel látja el,

b) az intézmény legalább napi gyakorisággal mentéseket készít a hitelesített tranzakciókról, és azokat az internetes informatikai rendszer üzemi környezetétől tűzbiztos módon és hozzáférés szempontjából is elkülönített, fizikai biztonságát tekintve is védett és ellenőrzött környezetben tárolja,

c) az intézmény a jogszabályi előírások szerinti ideig, de legalább 5 évig biztosítja a hiteles elektronikus tranzakciók adatainak visszakereshetőségét és hitelességük ellenőrizhetőségét.

11. Kriptográfiai eljárások és a kriptográfiai kulcsok kezelése

11.1. Megbízhatóknak csak azok a kriptográfiai algoritmusok tekinthetőek, amelyek nyilvánosak, azaz működési elvük mindenki számára szabadon hozzáférhető. Ezen algoritmusoknak a feltörhetetlenségét nem a titkosságuk biztosítja, hanem az, hogy matematikai törvényszerűségeken alapulnak, valamint hogy egy nyílt algoritmusnál a felhasználók biztosak

lehetnek abban, hogy nincs az algoritmusban hiba vagy kiskapu, amelyen keresztül beavatottak kulcs nélkül is hozzáférhetnek a nyílt adatokhoz, illetve azokat kulcs nélkül is módosítani tudják.

További biztonságot adhat az intézmények számára, ha olyan kriptográfiai eljárásokat alkalmaznak, illetve olyan algoritmus kódokat használnak, amelyeknek megfelelőségét független kriptográfiai szakérő, vagy tanúsító szervezet igazolta.

11.2 Az MNB javasolja, hogy az intézmény iparágilag elfogadott, biztonságos kriptográfiai eljárásokat és algoritmusokat, valamint dokumentált és teljes körű kulcs menedzsment eljárást alkalmazzon az interneten keresztül nyújtott pénzügyi tranzakciók azonosítása, rejtjelezése és hitelesítése során.

11.3. Előremutató gyakorlat

a) az informatikai rendszer kizárólag nyílt, iparágilag biztonságosnak elfogadott kriptográfiai eljárásokat és algoritmusokat alkalmaz[13],

b) a kriptográfiai kulcsok hosszúságát az intézmény a kulcsok élettartama szerint határozza meg, egy évnél hosszabb élettartam esetében a szimmetrikus kulcsok hossza legalább 256 bit, az aszimmetrikus kulcsok hossza legalább 2048 bit,

c) az intézmény teljes körű és dokumentált kriptográfiai kulcskezelési eljárással rendelkezik, és az megfelel valamelyik iparágilag elfogadott sztenderdnek, és kitér legalább az alábbiakra:

   i. biztonságos kulcselőállítás és kulcselosztás,

   ii. biztonságos kulcstárolás,

   iii. meghatározott időnkénti kulcscsere, lejárt élettartamú vagy feltételezhetően nyilvánosságra került kulcsok visszavonása, lecserélése,

   iv. kulcs megosztás és kettős hozzáférés (split knowledge & dual control) alkalmazása és annak módszere.

d) az informatikai rendszer kriptográfiai kulcsainak az előállítása és tárolása feltörés biztos hardver biztonsági modulban történik, amely kettős hozzáférés védelemmel (dual control) van védve az illetéktelen felhasználás ellen,

e) a titkos kulcsok és a magánkulcsok exportálása csak rejtjelezett formában lehetséges.

12. Az alkalmazások és a szoftver fejlesztése

12.1. Az interneten előforduló visszaélések jelentős részét az alkalmazások belső, a funkcionális működést nem zavaró – és így sokáig rejtett – tervezési hiányosságai vagy egyéb hibái – például a hibaágak- vagy a szokásos működés során nem bejárt feltétel ágak lezáratlanságai, kódolási hibák – teszik lehetővé. Ezeket kihasználva a támadók illetéktelen rendszer hozzáféréseket szereznek,

[13] az ajánlás készítésékor pl.: Blowfish, Twofish, Advanced Encryption Standard (AES, Rijndael), Serpent, RSA stb.

majd ezeken keresztül személyes haszonszerzés céljaira személyes adatokat vagy bank-biztosítási- fizetési- és értékpapír titok védelme alá tartozó adatokat tulajdonítanak el.

A tervezési hiányosságok elkerülésére – és ahhoz, hogy az internetes pénzügyi rendszer algoritmikus működése részleteiben is ellenőrizhető legyen – javasolt, hogy az internetes pénzügyi alkalmazások a nyílt, nemzetközi szinten egységesített sztenderdeket[14] használják.

Annak érdekében, hogy az alkalmazások minél kevesebb belső hibát tartalmazzanak, célszerű a kódolást olyan fejlesztőkkel végeztetni, akik ismerik az internetes alkalmazások szokásos sérülési pontjait, és járatosak a biztonságos internetes alkalmazásfejlesztési technikákban. Ezen túlmenően a rejtett hibák kiszűrését célszerű már az alkalmazás fejlesztés során, független programozók által elvégzett kód ellenőrzéseken keresztül elkezdeni, amely az elvárt színvonalú fejlesztői dokumentáció elkészítését is biztosíthatja.

Az alkalmazás belső hibáinak kiszűrésére javasolt elvégezni valamelyik nemzetközi web sérülékenységi tudásbázis[15] legfrissebb tartalma szerinti sérülékenységekre kiterjedő ellenőrzéseket is.

12.2. Az MNB javasolja, hogy az intézmény az internetes alkalmazások fejlesztése, illetve fejlesztetése során kövesse a nemzetközi ajánlásokat, gondoskodjon az alkalmazások kockázatokkal arányos teszteléséről, továbbá sérülékenység vizsgálatok elvégzésével igazolja az alkalmazások megfelelő védettségét.

12.3. Előremutató gyakorlat

a) az internetről elérhető webes alkalmazások architektúrája és működése megfelel a nemzetközi ajánlásoknak,

b) az alkalmazások fejlesztésével párhuzamosan elkészülnek a kód ellenőrzéseket is lehetővé tevő fejlesztői dokumentációk, valamint sor kerül a forrás programoknak a független személyek által elvégzett kódellenőrzésére,

c) az internetről elérhető pénzügyi alkalmazások tesztelése kiterjed az inputok, a hibaágak, valamint a szerepkörök szerinti hozzáférések teljes körű tesztelésére, valamint valamelyik nemzetközi web sérülékenységi adatbázis sérülékenységei szerinti ellenőrzésére is,

d) az internetről elérhető alkalmazások záró tesztjei kiterjednek az internetes kommunikáció, törési tesztekkel (penetration test) történő biztonsági ellenőrzésére is.

[14] pl. W3C, OASIS: XML, SOAP, WSDL, XAdES, XML Signature, XML Encryption, SAML, WS-Security, stb.

[15] pl. az OWASP TOP 10 vagy Common Weakness Enumeration

IV. Záró rendelkezések

13. Az ajánlás az MNB-ről szóló 2013. évi CXXXIX. törvény 13. § (2) bekezdés i) pontja szerint kiadott, a felügyelt pénzügyi szervezetekre kötelező erővel nem rendelkező szabályozó eszköz. Az MNB által kiadott ajánlás tartalma kifejezi a jogszabályok által támasztott követelményeket, az MNB jogalkalmazási gyakorlata alapján alkalmazni javasolt elveket, illetve módszereket, a piaci szabványokat és szokványokat.
14. Az ajánlásnak való megfelelést az MNB az általa felügyelt pénzügyi szervezetek körében az ellenőrzési és monitoring tevékenysége során figyelemmel kíséri és értékeli, összhangban az általános európai felügyeleti gyakorlattal.
15. Az MNB felhívja a figyelmet arra, hogy a pénzügyi szervezet az ajánlás tartalmát szabályzatai részévé teheti. Ebben az esetben a pénzügyi szervezet jogosult feltüntetni, hogy vonatkozó szabályzatában foglaltak megfelelnek az MNB által kiadott vonatkozó számú ajánlásnak. Amennyiben a pénzügyi szervezet csupán az ajánlás egyes részeit kívánja szabályzataiban megjeleníteni, úgy az ajánlásra való hivatkozást kerülje, illetve csak az ajánlásból átemelt részek tekintetében alkalmazza.
16. Az MNB a jelen ajánlás alkalmazását 2015. november 15-től várja el az érintett pénzügyi szervezetektől.
17. Hatályát veszti a Pénzügyi Szervezetek Állami Felügyeletének az internetbanki szolgáltatások biztonságáról szóló 7/2011. számú módszertani útmutatója, valamint az MNB-nek az internetbanki szolgáltatások biztonságáról szóló 2/2015. számú ajánlása.

Dr. Matolcsy György

a Magyar Nemzeti Bank elnöke