PÉNZÜGYI SZERVEZETEK
ÁLLAMI FELÜGYELETE
HUNGARIAN FINANCIAL
SUPERVISORY AUTHORITY

A Pénzügyi Szervezetek Állami Felügyeletének 7/2011. számú módszertani útmutatója az internetbanki szolgáltatások biztonságáról

Az internetbanki szolgáltatások biztonsága

Tartalom

A módszertani útmutató célja és hatóköre

Az internet alapú banki kiszolgálás a hitelintézetek tevékenységében ma már jelentős részt képvisel. Ugyanakkor az alkalmazott internetbanki megoldások – az internet jellegéből fakadóan – magas technológiai kockázatokat hordoznak magukban. Ezeket a kockázatokat az internetbanki alkalmazások esetében soha nem lehet teljes mértékben megszüntetni, hiszen az iparág és a technológia fejlődése gyors, ami önmagában hordozza a kockázatot, és ezért az internetbank szolgáltatóinak **folyamatos figyelme szükséges** ahhoz, hogy a kockázatokat kezelve, biztonságosan működtessék internetbanki szolgáltatásukat.

Jelen módszertani útmutató célja az interneten keresztül végzett banki műveletek biztonsága érdekében a nemzetközi „legjobb gyakorlat" alapján javasolható ajánlások és követendő gyakorlatok ismertetése és ezzel segítségnyújtás a hitelintézetek számára az internetbanki rendszerek elleni támadásokkal szembeni védekezésben.

Az útmutató tartalma – az internetes fenyegetettségek kettős irányultsága miatt – két részből áll, egyrészt az intézmények internetes szolgáltatásaival kapcsolatba hozható belső irányítási és üzemeltetési szabályokkal, másrészt pedig az internetbanki alkalmazások fejlesztési és belső biztonsági elemeivel foglalkozik.

Az útmutató nem befolyásolja a hitelintézeteknek – a rájuk egyébként vonatkozó – jogszabályi előírásoknak való megfelelési kötelezettségét, azok továbbra is érvényesek, betartandóak. Jelen útmutató ajánlásainak követése nem jogszabályon alapuló kötelezettség, de a Felügyelet tapasztalatai és véleménye szerint azok figyelembe vétele nélkülözhetetlen az internetes banki szolgáltatások biztonságos üzemeltetéséhez, valamint jelentős mértékben nyújt segítséget a hitelintézetek számára az informatikai biztonság jogszabályi követelményeinek teljesítéséhez.

Az ajánlások hatóköre

A módszertani útmutató címzettjei a hitelintézetek, de minden olyan pénzügyi szervezet számára iránymutató lehet, amely internet alapú kiszolgálást nyújt ügyfeleinek.

Jelen útmutatóban **internetbanki szolgáltatás** alatt az interneten keresztül indított és ügyfél számlákkal kapcsolatba kerülő műveletek kiszolgálását értjük. Az előremutató gyakorlatként feltüntetett ajánlások hatóköre az intézmények **internetbanki rendszerére** terjed ki, és magában foglalja az intézmények **internetbank hálózati környezetének** valamennyi rendszer elemét. **Internetbank hálózati környezet** alatt azokat az adathálózati szegmenseket kell tekinteni, amelyekben az internetbank szolgáltatás adatai megjelennek.

Az internetbanki szolgáltatásnak az alkalmazott kommunikációs közegtől és az ügyféloldali eszköz jellegétől függetlenül kell biztonságosnak lennie. Ezért az útmutató ezeket nem különbözteti meg, és egyaránt vonatkozik személyi számítógépekről, valamint hordozható (mobil) eszközökről – pl., mobilszolgáltatók hálózatát használó mobiltelefonokról vagy PDA-król – kezdeményezett internetbanki munkamenetek biztonságára.

Jelen útmutató a Felügyelet 1/2007. számú módszertani útmutatójához kapcsolódik (*„Pénzügyi Szervezetek Állami Felügyeletének 1/2007. számú módszertani útmutatója a pénzügyi szervezetek informatikai rendszerének védelméről"*), annak internetbanki biztonsági kiegészítéseként tekintendő.

Az útmutató készítése során figyelembe vett informatikai biztonsági ajánlások

Jelen módszertani útmutató a kiadása napján ismert fenyegetések figyelembe vételével készült, és tartalmában erősen támaszkodik az *MSZ ISO/IEC 27001:2006*, az *ISACA COBIT4*, az *ECBS Security Guidelines for E-banking (Application of Basel Risk Management Principles)* ajánlásokra, valamint a

vezető kártyatársaságok által kiadott – és PCI DSS néven ismert – *Payment Card Industry Data Security Standard v2.0* informatikai biztonsági követelmény rendszer előírásaira.

Az útmutatóban a kifejezések esetenként angol nyelven is történő jelzése a Felügyelet azon törekvését fejezi ki, hogy az elfogadott nemzetközi terminológia a lehető legpontosabban kerüljön közvetítésre a hitelintézetek számára.

1. Az internetbanki rendszerek irányítási környezete

1.1. Felsővezetői felügyelet

Az internetbanki rendszerek informatikai biztonsága érdekében a hitelintézeteknek azonosítaniuk kell az internetbank használatával szükségszerűen együtt járó kockázatokat, azok kezelésére ki kell dolgozniuk és alkalmazniuk kell a saját védelmi intézkedéseiket informatikai és biztonsági fejlesztések, eszközök és szabályozások formájában. Ehhez a várható támadási formák és lehetséges sérülékenységek rendszeres tanulmányozása is szükséges, hiszen az újabb és újabb fenyegetések újabb és újabb kockázatokat jelentenek a rendszerek működtetésére. A hibás működés és a visszaélések megelőzéséhez a technológiai biztonság megteremtésén túl kiemelten fontos szerepe van a felső vezetői irányításnak mind a védelmi intézkedések összehangolásában és ellenőrzésében, mind az internetbankkal kapcsolatos elvárások és intézkedések ügyfelek irányában történő képviseletében, megszemélyesítésében és az ügyfelek biztonság tudatosságának erősítésében.

Ajánlás

A hitelintézet felső vezetése alakítsa ki belső irányítási rendszerét vezetői elkötelezettség, folyamatba épített ellenőrzések, beszámoltatási-, valamint független ellenőrzési eljárások formájában. Biztosítsa, hogy a hitelintézeten belül valamennyi terület ismerje a saját felelősségét az internetbanki rendszerrel kapcsolatosan, kezelje a kockázatokat, valamint megtegye azokat a szükséges intézkedéseket, amelyekkel a felfedezett visszaélések elkövetői ellen hatékonyan fel lehet lépni.

Előremutató gyakorlat

A felső vezetés a felelősségi körében gondoskodik arról, hogy a hitelintézet:

- a technológiai kockázatok magas szintjéhez igazodóan folyamatosan figyelemmel kíséri az internetes fenyegetéseket, és új fenyegetések megjelenésekor valamint legalább évente egyszer átvizsgálja az internetbanki rendszerét, feltárja a működésben rejlő informatikai kockázatokat, továbbá gondoskodik a feltárt kockázatok kezeléséről,
- az internetbank által alkalmazott ügyfél azonosítási eljárás, valamint a tranzakciós adatok 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,
- rendelkezik azokkal a dokumentált eljárásokkal, amelyek biztosítják az internetbank rendszer visszamenőleges, egy korábbi állapotra történő szakértői vizsgálatának az elvégezhetőségét, és az eljárások megfelelőségét sikeres tesztekkel igazolja,
- csalásfelderítő – fraud monitoring – rendszert működtet az internetbank használatában előfordulható visszaélések visszaszorítására,
- az internetbanki szolgáltatás folyamatos rendelkezésre állásának biztosítására rendelkezik az előre nem tervezett rendszerkiesések kezelésére vonatkozóan, a feladatokat és a felelősöket is tartalmazó, az operatív tevékenységeket forgatókönyv-szerűen előíró üzletmenet-folytonossági és katasztrófa-elhárítási tervekkel, és ezek megfelelőségét sikeres tesztekkel igazolja,
- nyilvántartást vezet az internetbank szolgáltatással kapcsolatos biztonsági incidensekről és ügyfélpanaszokról, és elvégzi azok rendszeres kiértékelését és az internetbanki rendszer szükség szerinti korrekcióját.

1.2. Az ügyféloldal biztonság

Az internetbanki folyamatban az ügyfél magatartása, végfelhasználói eszközei jelentős kockázatot hordozhatnak. Az ügyfélkockázat a hitelintézetet is fenyegetheti, azonban számos harmadik forrásból érkező fenyegetést az ügyfél és a hitelintézet együttműködésével lehet hatékonyan kivédeni. Ennek eszköze lehet az ismeretterjesztés, az ügyfél-tájékoztatás, illetve ügyféloktatás.

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

Ajánlás

A hitelintézet az ügyféloldali biztonság megteremtésére folytasson hatékony ügyfél-tájékoztatási, oktatási tevékenységet a biztonságos internet használati ismeretek bővítésére.

Előremutató gyakorlat

- az ügyfél oldali biztonság kialakítása érdekében a hitelintézet tájékoztatást nyújt az ügyfelek felé a biztonságos internet használati ismereteik bővítésére. A tájékoztatás kitér legalább az alábbiakra:
    - a személyi azonosítók – különösen a jelszavak és a kriptográfiai magánkulcsok – használata, biztonságos kezelése,
    - vírusvédelem használatának jelentősége az ügyfél számítógépeken,
    - a hitelintézet internetes oldalának valódiságának ellenőrizésével az illetéktelen támadási kísérleteket kiszűrése – SSL kapcsolatok kiépülésének ellenőrzése, URL ellenőrzése, tanúsítványhiba megjelenése stb. –, az ellenőrzések elvégzésének fontossága,
    - megtévesztő tartalmú – pl. adathalász – e-mailek kiszűrése,
    - a bizalmas azonosító adatok elvesztése esetén követendő eljárások,
    - visszaélés észlelése vagy gyanúja esetén követendő eljárás,
    - a nem saját gépről történő, valamint a nyilvános internet pontokon[1] keresztüli internetbank használat veszélyeire, kockázataira való figyelem felhívása.
- a hitelintézet biztosítja az internet biztonsági bejelentések és kérdések folyamatos – 0-24 órás – fogadását, megválaszolását, valamint biztonsági intézkedések szakszerű és azonnali megtételének lehetőségét.

1.3. Az internetbanki rendszer belső hozzáférés-védelme, naplózása és a számonkérhetőség

Az informatikai rendszerek belső hozzáférés-védelmének alapfeladata a belső felhasználók azonosításával az illetéktelen felhasználók kizárása, továbbá a rendszerszintű jogosultsági beállításokon keresztül a felhasználók részére a rendszer-erőforrásokhoz való hozzáférések biztosítása olyan mértékben, amilyen mértékben az a munkájukhoz szükséges, és ezeken felül pedig – biztonsági okokból – a további erőforrás-hozzáférések tiltása. A felhasználók azonosításához és a jogosultságkezeléshez szükséges információk nyilvántartása ennek megfelelően az internetbanki rendszerek biztonságos működésének egyik meghatározó pontja.

[1] pl. wifi pontok, internet kávézók

A biztonságos rendszerüzemeltetéshez a hozzáférés korlátozás mellett utólagos ellenőrzés céljából szükséges a rendszerműködés, a rendszeresemények nyilvántartása, és a nyilvántartások megőrzése.

Ajánlás

A hitelintézet korlátozza az internetbank 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 internetbanki rendszer korábbi állapotaira vonatkozó szakértői vizsgálatok elvégezhetőségét.

Előremutató gyakorlat

- az internetbanki rendszeren belül az erőforrásokhoz való felhasználói hozzáférések korlátozva vannak azok számára, akiknek arra a napi munkájuk elvégzéséhez szükségük van, és a hozzáférési jogosultságok is korlátozva vannak a munkavégzéshez szükséges legalacsonyabb szintre,
- az internetbanki rendszerelemek hozzáférési jogosultsági beállításai biztosítják az internetbanki rendszer zártságát, azaz a felhasználók csak az alkalmazást használva férhetnek hozzá az internetbank rendszerek adataihoz, és a beállításokat a hitelintézet dokumentálja és rendszeresen ellenőrizi,
- külső partnerek által végzett tevékenységek minden esetben – akár lokálisan, akár távolról történnek – felügyelet alatt vannak tartva, és a végzett tevékenységeket az internetbanki rendszer naplózza úgy, hogy azok tartalma később visszamenőlegesen is megállapítható legyen,
- a távoli adatkapcsolatok esetileg, és csak a szükségességük idejére vannak felépítve, a tevékenység befejeződése után azonnal bontásra kerülnek,
- az internetbank környezethez való távoli hozzáférések esetében legalább kétfaktoros hálózati szintű hitelesítés működik,
- a felhasználói jelszavak hálózati átvitele valamint tárolása rejtjelezetten történik,
- valamennyi internetbanki rendszer és alkalmazás felhasználói jelszavainak – ideértve a kiemelt jogosultsággal rendelkező adminisztrátori jelszavakat is – kezelése az alábbiak szerint történik:
    - a kezdeti jelszavak egyediek, és kényszerítik a felhasználót az első bejelentkezéskor annak a megváltoztatására,
    - a 30 napja inaktív felhasználói azonosítók a rendszerben letiltásra kerülnek,
    - a felhasználói jelszavak megváltoztatása legalább 90 naponként kikényszerített,
    - a választható jelszavak a legutolsó 4 jelszótól különböznek,
    - a jelszavak hosszúsága legalább 7 karakter,
    - a jelszavak tartalmaznak kis- és nagybetűket és számokat is,
    - legalább 5 sikertelen belépési kísérlet után a felhasználói azonosító tiltásra kerül, és a kitiltás ideje legalább 5 perc vagy a rendszergazda újbóli engedélyezéséig tart.
- a technikai felhasználói azonosítók – pl. alkalmazások adatbázis felhasználói – kezelése biztonságos, azok legalább 8 karakter hosszúságúak, legalább 90 naponként megváltoztatásra kerülnek, és a hozzáférés védelmükre – pl. jelszómegosztással – teljesül a „négy szem elve”,
- az internetbanki szolgáltatás ügyfél által végrehajtott munkameneteinek banki tranzakciós folyamata naplózásra kerül,
- az internetbanki környezet komponenseire – felhasználói azonosítókkal és idővel azonosítottan – automatikus rendszeraudit naplózás működik legalább az alábbi tartalommal:

- a kiemelt – privilegizált, pl. a root vagy adminisztrátori – felhasználók tevékenységei,
- érvénytelen belépési kísérletek,
- sikertelen authorizációk eseményei (elutasított hozzáférési kísérletek),
- audit naplók újraindítása – inicializálása,
- rendszer objektumok létrehozása és törlése.

- a napló állományok védettek az illetéktelen módosítások ellen, ennek érdekében:
  - a naplóállományokért felelős rendszeradminisztrátorok valamint az internetbanki rendszerek üzemeltetését végző rendszeradminisztrátorok kölcsönösen ki vannak zárva egymás rendszereiből vagy
  - a napló bejegyzések utólagosan módosíthatatlan formában vagy módosíthatatlan adathordozóra azonnal rögzítésre kerülnek.
- napi gyakorisággal készülnek mentések a naplóállományokról, és azok az internetbank rendszer üzemi – éles – környezetétől tűzbiztos módon és hozzáférés szempontjából is elkülönítetten, fizikai biztonságát tekintve is védett és ellenőrzött környezetben megőrzésre kerülnek,
- a hitelintézet biztosítja a napló állományoknak a vonatkozó jogszabályokban előírt ideig, de legalább 5 évig történő visszakereshetőségét,
- az internetbanki rendszerkomponensek belső órái hiteles időszerverhez vannak – közvetlenül vagy közvetve – szinkronizálva.

1.4. Üzemeltetési biztonság

A Felügyelet a nemzetközi ajánlásokkal összhangban az internetbanki rendszerek üzemeltetésében magas informatikai biztonsági szint megvalósítását javasolja a hitelintézetek számára. A magas biztonsági szint megteremtése a szokásos informatikai biztonsági intézkedések magasabb biztonsági szinten történő megvalósítását, illetve azokon felül további védelmi intézkedések működtetését igényli.

Ezeket a – többlet – intézkedéseket a bevezetőben is meghatározottan az **internetbank 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 **internetbank hálózati környezete** alatt pedig azon hálózati szegmensek összességét tekintjük, amelyeken internetbanki adatok megjelennek.

A többlet intézkedések alkalmazása miatt az internetbank hálózati környezetet célszerű olyan kisméretűre kialakítani, amilyenre csak lehet. Ez megtehető, ha az internetbanki adatokkal érintett hálózatokat a hitelintézet 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.

Az adathálózat biztonsága

Ajánlás

A hitelintézet folyamatosan védje az internetbanki rendszerét tűzfal konfigurációval.

Előremutató gyakorlat

- az internetbank 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),
- az internetbank hálózati környezet internet felől elérhető eszközei – pl. a kommunikációs szerverei és website-jai – DMZ-ben, az internetbanki web szervizek és a banki alkalmazások, adatbázisok a DMZ mögötti belső hálózatokon kerülnek elhelyezésre,
- az internetbanki környezet DMZ zónái megfelelnek a DMZ definíciós előírásainak,
- a beállításokon keresztül a hitelintézet biztosítja, hogy csak indokolt és jóváhagyott tűzfal szabályok működnek, és ezeken felül a szabályrendszerek alapértelmezetten mindent tiltanak (deny all),
- megtörténik a tűzfal szabályok legalább 6 havonta történő felülvizsgálata és annak dokumentálása,
- a hitelintézet a nem biztonságos tűzfal szabályok esetében helyettesítő védelmi eljárásokat (kompenzációs kontrollokat) működtet,
- megtörténik a hálózati eszközök – routerek, tűzfalak, layer-3 + content switch-ek – konfigurációs fájljainak a mentése azok minden változtatását követően,
- a hitelintézet eljárást alakított ki és működtet a hálózati konfiguráció és a konfigurációs beállítások megváltoztatásának dokumentált jóváhagyására, tesztelésére és végrehajtására,
- amennyiben vezeték nélküli hálózatok kapcsolódnak az internetbank környezethez, azok tűzfal szabályrendszereken keresztül kapcsolódnak, biztonságos kriptográfiai protokollokat használnak[2] továbbá a vezeték nélküli hálózatok felől az internetbank környezet felé indított adatkapcsolatok tiltva vannak,
- az internetbank környezet határvédelme során mindenhol legalább állapotvizsgáló (dinamikus) csomagszűrő (stateful inspection) technológia működik,
- a hitelintézet az internetbank hálózati környezetére DoS/DDoS támadások elleni védelmet működtet.

<u>Biztonsági paraméter beállítások</u>

Ajánlás

A hitelintézet 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.

Előremutató gyakorlat

- az üzembe helyezésüket követően megtörténik az internetbanki rendszer elemek alapértelmezett jelszavainak és egyéb biztonsági paraméterei alapértelmezett beállításainak megváltoztatása,

[2] pl. WPA2

- valamennyi rendszerkomponens esetében a hitelintézet rendelkezik biztonsági házirenddel – biztonsági beállítási szabályzattal –, amely megfelel valamely elfogadott iparági „hardening” ajánlásnak[3], és a szabályzatokat rendszeresen frissíti,
- 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,
- a nem konzolról történő rendszeradminisztrátori kapcsolatok kriptográfiai rejtjelezéssel védettek.

Biztonságos rendszerek és alkalmazások használata

Ajánlás

A hitelintézet biztosítsa az internetbanki szoftveralkalmazások folyamatos és megbízható működését.

Előremutató gyakorlat

- az internetbanki rendszer elemeken antivírus rendszerek működnek. Ezek naprakész állapotúak, futnak és naplóznak. A beállításokon keresztül biztosított az automatikus frissítés, valamint teljes vírus ellenőrzések (on demand scan) rendszeres időszakonként – de legalább heti egy alkalommal – történő elvégzése,
- valamennyi internetbanki rendszer komponensre és szoftverre előzetes tesztelések elvégzését követően, de legfeljebb 60 napon belül installálásra kerülnek a gyártói javító csomagok,
- a rendszerkomponensek változtatásaira, új eszközök rendszerbe állítására teljes körű változáskezelési eljárás működik, a jóváhagyásokat a hitelintézet dokumentálja,
- a rendszer komponensek tesztelése úgy történik – pl. önálló, az üzemi környezettől elkülönített teszt környezet használatával –, hogy a tesztelés nem veszélyezteti az üzemi működést,
- az internetről elérhető web alkalmazások védelmére a hitelintézet minden változtatást követően, de legalább évente egy alkalommal kézi- vagy automatikus eszközzel sérülékenység vizsgálatot végez és gondoskodik arról, hogy a feltárt sérülékenységek javításra kerüljenek, vagy folyamatosan frissített web-alkalmazás tűzfalat (web application firewall) üzemeltet.

Biztonsági felügyeletek

Ajánlás

A hitelintézet az internetbank rendszer elemeinek audit naplóin keresztül folyamatosan ellenőrizze az internetbank rendszer üzemének megfelelőségét, valamint alkalmazzon technológiai megoldásokat az illetéktelen külső behatolások azonnali észlelésére vagy a támadások közvetlen elhárítására.

Előremutató gyakorlat

A hitelintézet

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

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

- legalább negyedévente wifi eszköz felderítést végez vagy vezeték nélküli behatolás felderítő eszközt (Wireless Intrusion Detection System) alkalmaz,
- változtatások után, de legalább negyedévente elvégzi az internetbanki rendszer elemek külső- és belső sérülékenység vizsgálatát (external/internal network vulnerability scan),
- változtatások után, de legalább évente elvégzi az internetbanki rendszer elemek törési vizsgálatát (penetration test),
- az internetbank környezet adatforgalmának ellenőrzésére behatolás-figyelő rendszert (Intrusion Detection System, IDS) vagy behatolás megakadályozó rendszert (Intrusion Prevention System, IPS) alkalmaz,

Incidenskezelés

Ajánlás

A hitelintézet készüljön fel a felügyeleti rendszerei által jelzett események – incidensek – kezelésére, ehhez dolgozzon ki hatékony incidenskezelési eljárást, az eljárást dokumentálja és annak megfelelőségét sikeres teszteredményekkel igazolja.

Előremutató gyakorlat

A hitelintézet

- rendelkezik az internetbanki szolgáltatásával kapcsolatosan dokumentált incidenskezelési eljárással, amely tartalmazza legalább az alábbiakat:
    - szerepek, feladatok, kommunikációs és kapcsolat felvételi stratégiák egy vélt vagy valós támadás, sérülés esetében,
    - részletes gyakorlati eljárások az antivírus és a felügyeleti rendszerek – pl. az IDS, IPS rendszerek – riasztásainak kezelésére,
    - részletes gyakorlati eljárások a (D)DoS támadások kezelésére,
    - tesztelési eljárások az incidenskezelés megfelelőségének ellenőrzésére.
- legalább évente elvégzi és dokumentálja incidenskezelési eljárásainak tesztelését.

Szolgáltatók igénybe vétele

Ajánlás

Annak érdekében, hogy azok ne jelentsenek szükségtelen kockázatot, a hitelintézet az internetbanki szolgáltatásához igénybe vett szolgáltatók kiválasztását, valamint az együttműködés feltételeinek a kialakítását az internetbanki kockázatok mértékéhez illeszkedően, kiemelt gondossággal végezze[4].

Előremutató gyakorlat

- a hitelintézet a szolgáltató kiválasztását megelőzően meggyőződik arról, hogy a szolgáltató informatikai biztonsági szintje a tevékenységet illetően megfelel-e legalább a hitelintézetekre vonatkozó előírásoknak, illetve nem alacsonyabb-e a saját biztonsági szintjénél,
- a hitelintézet az internetbanki szolgáltatás területén igénybe vett szolgáltatókkal megkötött szerződéseiben a szolgáltatásra vonatkozóan:

[4] Amennyiben a hitelintézet a szolgáltatót kiszervezett tevékenység elvégzésére veszi igénybe, feleljen meg teljeskörűen a Hpt. 13/A.§ (Kiszervezés) előírásainak is.

- egyértelműen meghatározza a szolgáltatási szinteket, azok mérési eljárásait, valamint a szolgáltató nem szerződésszerű teljesítésének eseteire vonatkozó feltételeket,
- egyértelműen meghatározza a szolgáltató által felvállalt információbiztonsági felelősséget,
- kiköti a hitelintézet helyszíni, illetve helyszínen kívüli ellenőrzési jogát, ami kiterjed a szolgáltató alvállalkozóira is,
- rögzíti, hogy alvállalkozót a szolgáltató csak a hitelintézet jóváhagyásával alkalmazhat,
- rögzíti a szolgáltató és esetleges alvállalkozói felelősségét a tevékenység megfelelő színvonalon történő végzéséért, valamint a hitelintézet azonnali felmondási lehetőségét a szerződés ismételt vagy súlyos megszegése esetére.

- a hitelintézet folyamatosan felügyeli a szolgáltatások szerződésszerű teljesítését.

1.5. Üzletmenet-folytonosság biztosítása

Az internetbanki szolgáltatásokkal szemben is elvárás, hogy azok legyenek folyamatosan elérhetők az ügyfél-megbízások befogadására, és legyenek alkalmasak az internetbank nyitvatartási ideje alatt a megbízások teljesítésére.

Ajánlás

Az ügyfélbizalom, valamint az ügyfél-kiszolgálás színvonalának fenntartása érdekében a hitelintézet alkalmazzon olyan műszaki-technológiai megoldásokat, amelyek csökkentik az internetbanki rendszerek elérhetőségének, valamint az internetbanki szolgáltatás kiesésének lehetőségét, illetve rendelkezzen azokkal a tartalék eszközökkel illetve megoldásokkal, amelyek a nem várt kiesések eseteire biztosítani tudják az internetbanki szolgáltatásnak – a hitelintézet által elvárt helyreállítási idők alatti – újraindíthatóságát.

Előremutató gyakorlat

- a hitelintézet adathálózata redundáns, azaz nem tartalmaz „single point of failure” rendszer elemet,
- az internetbanki szolgáltatás kiesésének lehetséges eseteire vonatkozóan a hitelintézet a szolgáltatás indítását megelőzően meghatározza azokat az – üzletileg még elfogadható – helyreállítási időket, amelyeken belül az internetbank szolgáltatás újra indulását elvárja, ezeket az időket a szolgáltatásában bekövetkező változások esetén minden esetben felülvizsgálja,
- a hitelintézet rendelkezik azokkal a tartalék eszközökkel vagy tartalékolási megoldásokkal, amelyekkel az elvárt helyreállítási időn belül az internetbank működése helyreállítható,
- a hitelintézet felkészült az internetbanki 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,
- gyakorlati tesztek sikeres elvégzéseivel a hitelintézet igazolta, hogy az internetbank szolgáltatást az elvárt helyreállítási időkön belül újra tudja indítani.

2. Internetbanki alkalmazások

2.1. Az ügyfél azonosítása

Az internetbanki alkalmazások meghatározó kockázati pontja az ügyfél személyazonosságának távoli – az interneten keresztül történő – meghatározása. Az internetbanki kapcsolat kezdeményezőjének azonosítása többféle módon és többféle biztonsági szinten történhet. Egyfaktoros azonosítás esetében az ügyfélhez rendelt felhasználói azonosító és a hozzátartozó (statikus) jelszó alapján történik meg az azonosítás, többfaktoros azonosítás esetében kettő- vagy több személyi azonosító adatot használ az azonosítási folyamat, a magas biztonságot nyújtó PKI technológia alkalmazása esetén pedig az ügyfél azonosítása kriptográfiai tanúsítványával történik.

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

A többfaktoros azonosítás esetében 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 pl.:

- az ügyfélhez az internetbanki kapcsolatától biztonsági szempontból elkülönülő (out of band) másik kommunikációs csatornán (pl. SMS-ben) eljuttatott, egyszeri, véletlenszerű és időkorlátos azonosító adat – a dinamikus jelszó,
- PIN kóddal vagy jelszóval védett kód előállító eszköz – pl. hardver token –által előállított időkorlátos véletlenszerű számsorozat – a dinamikus kód,
- TAN kód (transaction authentication number), az ügyfélnek korábban kiadott, egyszeri alkalommal használható azonosító kódok halmaza,
- az ügyfél személyazonosságának telefonon keresztül történő hitelesítése.

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 azonosítására.

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

- sikeres és/vagy sikertelen bejelentkezésről, tranzakciókról SMS/email üzenetet küldhetnek a felhasználók számára,
- virtuális billentyűzetet használhatnak az azonosítók bevitelére,
- ismételt sikertelen bejelentkezési kísérleteket követő sikeres bejelentkezéskor captcha[5]-t alkalmazhatnak.

[5] 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)

Pénzügyi kötelezettségeket jelentő műveletekhez PKI technológia alkalmazása vagy legalább kétfaktoros hitelesítés használata szükséges. A hitelintézet egy időben többféle azonosítási módszert is használhat annak függvényében, hogy az ügyfél milyen műveleteket – és milyen tranzakciós limitekkel – hajthat végre az interneten keresztül.

Ajánlás

A hitelintézet internetbank rendszere az ügyfélkapcsolat létesítéséhez végezzen ügyfél azonosítást. Ennek során az alkalmazott azonosítási módszer biztonságossága legyen arányos a végezhető internetbanki műveletek kockázataival. Pénzügyi kötelezettséget jelentő műveletekhez PKI technológia alkalmazása – és ennek részeként biztonságos hozzáférés védelemmel rendelkező aláírás-létrehozó eszköz használata – elvárt, de ennek hiányában is legalább kétfaktoros hitelesítési módszer alkalmazása szükséges.

Előremutató gyakorlat

- a internetbanki rendszer olyan ügyfél azonosítási eljárást alkalmaz, amelynek biztonságossága arányos a végezhető banki műveletek kockázataival,
- a hitelintézet az ügyfél kapcsolat kezdeményezésekor biztonságos kommunikációs csatornát épít ki, az ügyfél azonosítást ezen keresztül végzi, és a biztonságos csatornát (transport layer) a munkamenet végéig fenn tartja (pl. SSL/TLS, IPSEC),
- a hitelintézet szervertanúsítványának érvényességi láncában szerepel az ismert böngészőkben is telepített valamelyik tanúsítvány-kiadó szervezet,
- 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,
- statikus jelszavak használata esetében a hitelintézet (legalább) az alábbi védelmi intézkedéseket alkalmazza:
    - sikertelen belépési kísérletet követően az ügyfél felhasználói azonosítójának az automatikus kitiltása legalább 10 másodpercre,
    - sikertelen belépési kísérletekre vonatkozó figyelem felhívás küldése az ügyfél felé legalább a következő sikeres belépésekor.
- a független csatornán eljuttatott dinamikus jelszó csak az operatív memóriában, és csak a vele történő műveletvégzés idejére kerül tárolásra, utána törlődik, ismételt felhasználáshoz azt az internetbanki rendszer az ügyféltől ismételten bekéri,
- a független csatornán eljuttatott dinamikus jelszó élettartama nem több mint 10 perc,
- a dinamikus kód élettartama nem több mint 1 perc,
- az ügyfél azonosító adatok hitelintézet általi kezelése felügyelet és ellenőrzés alatt tartott, és kizárt az egyszemélyi visszaélés lehetősége,
- az ügyfél előzetes kérése alapján a hitelintézet azonnali értesítéseket küld számára internetes számlája egyenlege, valamint személyi azonosító adatai változásakor.

2.2. A tranzakciós üzenetek végponti védelme

Az internetbanki műveletvégzés során – az ügyfél és az internetbanki kommunikációs web site-ok között kiépülő biztonságos csatorna (pl. SSL/TLS, IPSEC) használata mellett biztosítani kell az internetbanki tranzakciós üzenetek védelmét az ügyfél valamint az internetbanki web szervizek – mint üzenetvégpontok – között is (end to end, vagy message security). A végponti védelem során biztosítani kell az alábbi négy biztonsági tényező teljesülését:

1. a bizalmasságot, azaz a tranzakciós üzenetek lehallgatás elleni védelmét,
2. a sértetlenséget, azaz tranzakciós üzenetek módosítások elleni védelmét,
3. a hitelességet, azaz a tranzakciós üzenetek küldőjének hitelesítését,
4. valamint a letagadhatatlanságot, azaz az üzenetküldés tényének a letagadhatatlanságát.

Ezek teljesítéséhez a PKI technológia és az ügyféloldalon elektronikus aláírás használata szükséges. 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.

Szimmetrikus rejtjelezés használatával a tranzakciós üzenetek bizalmassága, sértetlensége biztosítható, az üzenetküldő hitelesítése az üzenetküldő tulajdonát képező valamely adatnak – pl. dinamikus jelszó vagy dinamikus kód – az üzenethez rendelésével valósítható meg. Az üzenet sértetlenségének az ellenőrzése ebben az esetben megvalósítható pl. kriptográfiai ellenőrző összeg (Message Authentication Code, MAC - cryptographic checksum) használatával, de az üzenetküldés letagadhatatlansága önmagában szimmetrikus kulcsok használatával nem biztosítható.

A hitelintézetnek a letöltésre kerülő beépülő kriptográfiai modulok sértetlenségét és hitelességét is biztosítania kell.

Ajánlás

A hitelintézet internetbanki rendszere valósítsa meg az internetbanki tranzakciós üzenetek végponti védelmét, ennek során biztosítsa a tranzakciós üzenetek bizalmasságát, sértetlenségét és hitelességét, valamint biztosítsa az üzenetküldés letagadhatatlanságát.

Előremutató gyakorlat

- a hitelintézet az internetbanki tranzakciók bizalmasságát és integritását kriptográfiai rejtjelezéssel biztosítja,
- a hitelintézet az üzenetküldő hitelesítésére az ügyfél birtokában már meglévő, vagy neki az internetbanki 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,
- a TAN kód, a dinamikus kód legalább 6, a dinamikus jelszó legalább 8 karakter hosszúságú,
- a hitelintézet a tranzakciós üzenetek sértetlenségének a megállapítására az üzeneteket elektronikus aláírással vagy kriptográfiai ellenőrző összeggel (cryptographic checksum) látja el,
- a hitelintézet 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,
- a hitelintézet a tranzakciós üzenetek védelmére eseti üzenet azonosítókat (security token) használ,
- az eseti üzenetazonosítók élettartama nem több mint 10 perc,
- amennyiben vannak letöltődő kliens szoftverek, beépülő modulok (java appletek, active-x modulok), azok a hitelintézet által elektronikusan alá vannak írva.

2.3. Az elektronikus tranzakciók megőrzése

Az internetbanki műveletek bizonylatai – a papír alapú megbízások hiányában – az elektronikus tranzakciók. Szükséges, hogy a hitelintézet az elektronikus tranzakciókat a forgalmazásuk időpontjával együtt hitelesen megőrizze. A hiteles tranzakció állomány alapján tudja a hitelintézet

később vizsgálni – adott esetben bizonyítani –, hogy egy banki tranzakció forrása internet felől beérkezett elektronikus tranzakció volt-e.

Az elektronikus tranzakciók 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 a bizonyító ereje – a rendszer állományok módosíthatóságától, illetve a módosítások elleni védettségétől, és annak hiteles biztosításától függ.

A tranzakciók hitelességének az igazolhatóságára az internetbanki rendszer az elektronikus tranzakciókat elektronikus aláírással és időbélyeggel láthatja el. Az időbélyeget a hitelintézet saját maga, vagy külső – esetleg minősített – időbélyegzés-szolgáltató készítheti.

Ajánlás

A hitelintézet hitelesítse az elektronikus tranzakciós üzeneteit, gondoskodjon azok biztonságos őrzéséről, valamint biztosítsa a jogszabályokban előírt ideig, de legalább 5 évig azok visszakereshetőségét és hitelességük igazolhatóságát.

Előremutató gyakorlat

- a hitelintézet az internetbanki tranzakciós üzeneteket elektronikus aláírással és időbélyeggel látja el,
- a hitelintézet által alkalmazott időbélyegzés megfelel a minősített időbélyegzés-szolgáltatásra vonatkozó jogszabályok biztonsági követelményeinek, ennek hiányában a hitelintézet minősített időbélyegzés-szolgáltatót alkalmaz,
- a hitelintézet legalább napi gyakorisággal mentéseket készít a hitelesített tranzakciókról, és azokat az internetbank rendszer üzemi környezetétől tűzbiztos módon és hozzáférés szempontjából is elkülönített, fizikai biztonságát tekintve is védett és ellenőrzött környezetben tárolja,
- a hitelintézet a jogszabályi előírások szerinti ideig, de legalább 5 évig biztosítja a hiteles elektronikus tranzakcióknak a visszakereshetőségét és hitelességük ellenőrizhetőségét.

2.4. Kriptográfiai eljárások és a kriptográfiai kulcsok kezelése

Megbízhatóaknak 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 a hitelintézetek számára, ha olyan kriptográfiai eljárásokat alkalmaznak, illetve olyan algoritmus kódokat használnak, amelyeknek megfelelőségét független kriptográfiai szakérő, vagy tanúsító szervezet igazolta.

Ajánlás

A hitelintézet iparágilag elfogadott, biztonságos kriptográfiai eljárásokat és algoritmusokat, valamint dokumentált és teljes körű kulcs menedzsment eljárást alkalmazzon az internetbanki tranzakciók azonosítása, rejtjelezése és hitelesítése során.

Előremutató gyakorlat

- az internetbank rendszer kizárólag nyílt, iparágilag biztonságosnak elfogadott kriptográfiai eljárásokat és algoritmusokat használ[6],
- a kriptográfiai kulcsok hosszúságát a hitelintézet 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,
- a hitelintézet teljes körű és dokumentált kriptográfiai kulcskezelési eljárással rendelkezik, és az megfelel valamelyik iparágilag elfogadott sztenderdnek, és kitér legalább az alábbiakra:
    - biztonságos kulcselőállítás és kulcselosztás,
    - biztonságos kulcstárolás,
    - meghatározott időnkénti kulcscsere, lejárt élettartamú vagy feltételezhetően nyilvánosságra került kulcsok visszavonása, lecserélése,
    - kulcs megosztás és kettős hozzáférés (split knowledge & dual control) alkalmazása és annak módszere.
- az internetbanki 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,
- a titkos kulcsok és a magánkulcsok exportálása csak rejtjelezett formában lehetséges. A rejtjelezésre használatos kulcsrejtjelező kulcs (key encryption key, master key) előállítása és tárolása a hardver biztonsági modulban történik. Amennyiben – pl. mentési okokból – a kulcsrejtjelező kulcs exportálására kerül sor, az csak a kulcs részekre osztása mellett történik oly módon, hogy az egyes kulcs részeket más és más kulcs gazdák – és csakis ők – ismerhetik meg. Az exportálások során a kulcsok részekre osztását és a kulcs gazdák hitelesítését a hardver biztonsági modul végzi.

  Az exportálást követően a hitelintézet különleges figyelmet fordít arra, hogy a kulcsrejtjelező kulcsok későbbi használata során teljesüljön a „4 szem elve”.

2.5. Az alkalmazások és a szoftver fejlesztése

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, majd ezeken keresztül személyes haszonszerzésük céljaira személyes adatokat vagy bank- és értékpapír titok védelme alá tartozó adatokat tulajdonítanak el.

A tervezési hiányosságok elkerülésére – és ahhoz, hogy az internetbanki rendszer algoritmikus működése részleteiben is ellenőrizhető legyen – javasolt, hogy az internetbanki alkalmazások a nyílt, nemzetközi szinten egységesített web szolgáltatási protokollokat, leírókat és sztenderdeket[7] használó web szervizek legyenek.

Annak érdekében, hogy az alkalmazások minél kevesebb belső hibát tartalmazzanak, célszerű a fejlesztést olyan fejlesztőkkel végeztetni, akik ismerik az internetes alkalmazások szokásos sérülési pontjait, és járatosak a biztonságos internetes alkalmazásfejlesztési technikákban. Ezen túlmenően a

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

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

rejtett hibák kiszűrését célszerű már az alkalmazás fejlesztés során, független programozók által elvégzett kód ellenőrzéseken keresztül elkezdeni, ez egyébként az elvárt színvonalú fejlesztői dokumentáció elkészítését is biztosíthatja.

Az alkalmazás belső hibáinak kiszűrésére javasolt elvégezni valamelyik nemzetközi web sérülékenységi adatbázis[8] legfrissebb tartalma szerinti sérülékenységekre kiterjedő ellenőrzéseket is.

Ajánlás

Az internetbanki rendszer működését web szervizek valósítsák meg, továbbá a hitelintézet az internetbanki alkalmazások fejlesztése, illetve fejlesztetése során gondoskodjon az alkalmazásoknak az internetes kockázatokkal arányos teszteléséről, továbbá igazolja sérülékenység vizsgálatok elvégzésével az alkalmazások védettségét.

Előremutató gyakorlat

- az internetbanki webes alkalmazások architektúrája és működése megfelel a nemzetközi web szerviz ajánlásoknak,
- az alkalmazások fejlesztésével párhuzamosan elkészülnek a kód ellenőrzéseket is lehetővé tevő fejlesztői dokumentációk, valamint sor kerül a kódok független személyek által elvégzett kódellenőrzésére,
- az internetbanki alkalmazások tesztelése kiterjed az inputok, a hibaágak, valamint a szerepkörök szerinti hozzáférések teljes körű tesztelésére, valamint valamelyik nemzetközi web sérülékenységi adatbázis sérülékenységeinek az ellenőrzésére is,
- az internetbanki alkalmazások záró tesztjei kiterjednek az internetes kommunikáció védettségének törési (penetration) tesztekkel történő ellenőrzésére is.

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