FOTÓ: IT-SECURITY

Bognár Zsolt,
senior tanácsadó, Triad Kft.

Legalább úgy, mint papíron

Egy-egy elektronikus számlával kapcsolatos műveletben több szereplő is részt vesz, s adataik védelmét, a biztonságot mindannyiuk számára garantálni kell.

– Több helyen olvashattunk a Távszámla szolgáltatás előnyeiről – a szolgáltatónál jelentkező megtakarításokról, az ügyfél által tapasztalt gyorsaságról és kényelemről. A biztonsági vonatkozásokról azonban nemigen hallhattunk.

– Márpedig ilyenek bőven vannak, hiszen pénzről, pénz értékű dokumentumokról, fizetési lehetőség megteremtéséről van szó. Az sem mellékes, hogy a számlák sokat elmondhatnak valakinek a fogyasztói szokásairól, magán- (vagy éppenséggel vállalati) életéről. Így ahhoz, hogy egyáltalán, a világon bárhol meg lehessen valósítani az elektronikus számlabemutatás és -fizetés [közkeletű angol rövidítéssel Electronic Bill Presentment and Payment, EBPP] remek ötletét, egy sor biztonsági problémát át kellett látni, meg kellett oldani.

A legnagyobb „kár” az lehet, hogy valaki kifizeti a számlámat

– A múlt idő azt is jelenti, hogy a következőkben valóban megoldott kérdésekről beszélgetünk?

– Igen. Szolgáltató és ügyfél egyaránt nyugodt lehet: napjainkra olyan elvek és módszerek kristályosodtak ki, amelyek biztonsága, védettsége semmiben sem marad el a hagyományos, papír alapú számlázásétól. Legalábbis az EBPP-piacon messze vezető amerikai CheckFree esetében – amelynek technológiáján például az említett Távszámla is alapul – ez mindenképpen elmondható. Érezte ezt a jogalkotó is, különben nem születhetett volna meg a 20/2004-es PM-rendelet, amely megteremtette az EBPP hazai bevezetésének törvényi kereteit.

Hozzáteszem: az egyik cél, amely a fejlesztők szeme előtt lebegett, pontosan az volt, hogy a rendszerek sem az esetleges betörések számára, sem pedig jogi szempontból ne nyújtsanak nagyobb támadási felületet, mint a papír alapú folyamatok. Így aztán több szempontból modellnek is tekintették a nyomtatott számlák kezelésében kialakult, jól bevált gyakorlatot.

Kik az EBPP-tér szereplői? Az nyilvánvaló, hogy a rendszerrel kapcsolatban áll egy vagy – ideális esetben – több számlakibocsátó (mondjuk távközlési társaság vagy közmű), s hogy a fizetések elektronikus teljesítéséhez szükség van egy bankra is. Kevésbé evidens azonban – jóllehet biztonsági szempontból igen lényeges –, hogy a rendszer felhasználója, a számlakibocsátóval szerződéses viszonyban álló fogyasztó és a fizetéshez igénybe vett bankszámla vagy -kártya tulajdonosa nem feltétlenül ugyanaz a személy.

FOTÓ: IT-SECURITY

Hogy egy sárga csekket ki fizet be s kinek a pénzével, az a számlakibocsátó számára közömbös: neki csak az a fontos, hogy befolyjon a kért összeg. Meglehet persze, hogy én magam adom fel a postán a saját nevemre érkezett telefonszámlát, s ehhez a pénzt a saját bankszámlámról vettem fel. De az sem ritka, hogy egy családfő több, különböző névre szóló számlát egyenlít ki, sőt az is előfordulhat, hogy ehhez például a nagymama bankszámláját veszi igénybe.

Nincs ez másként az EBPP esetében sem. Elvi szempontból mindenképpen meg kell tehát különböztetnünk a szolgáltatóval kapcsolatban lévő fogyasztót, a banki ügyfelet és az EBPP-rendszer felhasználóját – vagyis azt, aki egy portálra bejelentkezve ténylegesen elektronikusan meg akarja jeleníteni, vagy ki szeretné fizetni a számlát.

– Ha elvben elkülönítik őket, akkor ez a gyakorlatban is bizonyára tükröződik.

– Az EBPP-vel összefüggő biztonsági feladatok egyik nagy csoportját éppen a szereplők adatainak szétválasztott kezelése jelenti. Nem lehet átjárás az egyes számlakibo-

csátók adatai között (azaz például a telefontársaság nem nézheti meg a gázszámlát és viszont), a bank és a számlakibocsátók adatai között, de a banki ügyfél, a fogyasztó és az EBPP-rendszer felhasználójának adatai között sem.

A banknak még az ügyfél bankszámlaszámát sem kell feltétlenül átadnia az EBPP-központnak. Tökéletesen megfelel egy, a rendszer konvenciójához illeszkedő referencia. Ugyanez a helyzet a számlakibocsátóval is: ha akarja, az EBPP-portálon maga jelenítheti meg az adatokat egy önálló, általa szolgáltatott keretben, illetve a fogyasztó belső azonosítóját sem kell kiadnia az EBPP-központ számára – elegendő ehelyett egy 1:1 megfeleltetést biztosító belső kód.

Hogy befejezzem a szétválasztás témáját: arról se feledkezzünk meg, hogy az egyes felhasználók sem láthatnak bele egymás adataiba.

– Ahhoz viszont, hogy beláthassanak a nekik szóló információba, előbb jogosultság-ellenőrzésre van szükség.

– Így van. Adatszétválasztás és jogosultságkezelés két egymással szorosan összefüggő terület. Az EBPP-rendszer nem kíváncsi a felhasználó személyi adataira. Szolgáltatói oldalról a központnak az kell, hogy tudja: melyik számlakibocsátónál milyen fogyasztóazonosítóval tartják nyilván azt, akinek a számláiba betekintést kell adni, illetve akinek a számláit ki akarják fizetni.

Hasonlóképpen: banki oldalról a fizetés fedezetéül szolgáló bankszámla vagy -kártya számára van szükség.

– Honnan tudja a számlakibocsátó, hogy csakugyan az kér tőle EBPP-belépést, aki erre fogyasztóként jogosult?

– Biztonsági szempontból a legegyszerűbb a hagyományos, papír alapú eljárás leutánzása. A számlakibocsátó felveszi az online érkezett igényt. Az igény közléséhez elegendő az ügyfélnek a számlán szereplő fogyasztóazonosítót megadnia. Ennek birtokában a számlakibocsátó adatbázisából kikeresi az ügyfél nevét és lakcímét, majd (postai, hagyományos) levelet küld az adott névre és címre, s ebben megadja az EBPP-rendszerben használandó egyedi azonosító kódot. Az addig függőben lévő EBPP-megállapodás abban a pillanatban „aktiválódik”, amint az ügyfél a portálon a postai úton kapott kóddal aktiválja azt.

Az aktiválással életbe léptetett szerződés addig hatályos, míg azt valamelyik fél fel nem mondja. Ez leginkább olyankor fordul elő, amikor az ügyfél elköltözik, vagy valamely szolgáltatást nem vesz tovább igénybe.

Az elektronikus rendszer biztonsága semmivel sem kérdőjelezhetőbb meg jobban, mint a hagyományosé. A két szisztéma azonos szintű védelmet, garanciákat nyújt. A szolgáltatók más regisztrációs folyamatot is kialakíthatnak, amelyek akár nagyobb biztonságot is kínálhatnak.

FOTÓ: IT-SECURITY

Mindenesetre nem kis dolog, hogy némi éllel kimondhatom: a legnagyobb kár, ami az EBPP-ben érhet, hogy valaki akaratom ellenére kifizeti a számlámat.

– Mi történik a kifizetésekkel?

– Gyakorlatilag ugyanez. Ott nem fogyasztóazonosítót, hanem bankszámla- vagy -kártyaszámot kell hasonló módon megadnia az ügyfélnek. (Ismét hangsúlyozom: lehet, hogy nem a fogyasztó, hanem más személy áll a bankkal szerződéses viszonyban.) Persze a pénzintézeti szabályozás szigorúbb szokott lenni, így könnyen meglehet, hogy az illetőnek személyesen be kell fáradnia egy bankfiókba ahhoz, hogy EBPP-megbízást adjon.

Nem lehet átjárás az egyes számlakibocsátók adatai között

Azért nem fogalmaztam határozottabban, mert az ügyfelek nem kis részének ma már internetbanki megállapodása is van. Ha pedig egyszer már létezik egy ilyen, kölcsönösen megbízhatónak tekintett csatorna a bank és az adott személy között, akkor azt az utóbbi arra is használhatja, hogy EBPP-felhatalmazást adjon.

Egy esetre még érdemes kitérni. Míg az nagyon gyakori, hogy a fogyasztó és az EBPP-rendszer felhasználója két különböző személy, a bankszámla-tulajdonos általában azonos a felhasználóval. Kicsit közérthetőbben: az szokott EBPP-rendszerbe bejelentkezni, aki amúgy is intézi a család pénzügyeit. Miután nem egy esetben az EBPP-szolgáltatásokkal kiegészített portált valamelyik bank üzemelteti, az utóbbi esetben lényegesen leegyszerűsödik az azonosítás, hiszen egy már nyilvántartott banki ügyfélnek kell jogosítványt adni a pénzintézet egy másik szolgáltatásának a használatára.

Ez akkor is igaz, ha magát az EBPP-szolgáltatást nem a bank üzemelteti, hanem csak közvetíti azt. Ilyenkor azonban senki sem szereti, ha egyetlen ügy elintézéséhez kétszer-háromszor kell különböző helyeken bejelentkeznie, így nagy előny, ha egyszeri belépést tudunk biztosítani az ügyfélnek a rendszerek közötti biztonságos átjárás megteremtéséhez.

– Meglepődtem, hogy eddig szóba sem kerültek olyan fogalmak, mint a behatolásvédelem vagy a titkosítás.

– Ennek egyszerűen az az oka, hogy mindvégig az EBPP-koncepcióhoz kapcsolódó speciális biztonsági megfontolásokról beszéltem. Ám természetesen mindaz, amit az internetes biztonság területén eddig kifejlesztettek, azt az EBPP-ben is alkalmazni kell, s a cégek fel is vonultatják a teljes kelléktárat.

Adatbázis-szinten a legérzékenyebb információkat titkosítottan – nyilvános kulcsos rendszerben – szokás tárolni, hogy ezáltal is erősödjék a védelem. Az alkalmazási rétegben célszerű felhasználói profilokat felállítani, s a felhasználókat csoportosítani.

Ez utóbbi gyakorlatot már csak azért is fontosnak tartom megemlíteni, mert ily módon gyorsabb lehet a rendszer. Márpedig ha az erőforrásokat folyamatosan a védelem, az ellenőrzés köti le, az nem megoldás. Hiszen a biztonság nem öncél, hanem – esetünkben – a számlamegjelenítés és fizetés egyik szükséges eszköze, feltétele.

Mikolás Zoltán