HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

KIBERBIZTONSÁGI VÁLTOZÁSOK A FIZETÉSI SZOLGÁLTATÁSOKNÁL

CYBERSECURITY CHANGES IN THE PAYMENT SERVICES

SZÁDECZKY Tamás; VÁCZI Dániel

(ORCID: 0000-0001-7191-4924); (ORCID: 0000-0001-6770-6954)

szadeczky.tamas@uni-nke.hu; vaczi.daniel@hotmail.com

Absztrakt

A tanulmányban elemezzük a fizetési szektort a jövőben várhatóan jelentősen megváltoztató Payment Services Directive 2 (PSD2) Európai Uniós irányelvet. Megvizsgáljuk az előzményeit, a létrejöttének hátterét, és a várható hatását a fizetési szolgáltatások informatikai biztonságára. A szakma által sok pontban vitatott irányelvvel kapcsolatban megvizsgáltuk a főbb lefedett témaköreit, különös tekintettel az emberi tényezőre, mint e rendszer gyenge láncszemére.
Szembe állítjuk ezzel a jelenleg hatályos bankkártyás fizetésre vonatkozó szabályozás, a Payment Card Industry Data Security Standard (PCI DSS) különböző információbiztonsági előírásait.
Az Emberi Erőforrások Minisztériuma ÚNKP-17-4-III-NKE-26 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.

Kulcsszavak: *PSD2, PCI DSS, elektronikus fizetés, bankkártya, hitelkártya, információbiztonság*

Abstract

In our paper, we are analyzing the European Union's Payment Services Directive 2 (PSD2), which will probably change the payment sector shortly. We investigated its predecessors, background and its probable impact on the information security of payment services. We examined the main topics discussed in the directive, including the human factor as a weak element of the security.
We are comparing the PSD2 with the information security requirements of the Payment Card Industry Data Security Standard (PCI DSS), which is the current regulation defining the rules of credit card payment.
Supported by the ÚNKP-17-4-III-NKE-26 New National Excellence Program of the Ministry of Human Capacities.

Keywords: *PSD2, PCI DSS, electronic payment, bank card, credit card, information security*

A kézirat benyújtásának dátuma (Date of the submission): 2018.06.06.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.25.

BEVEZETÉS

A 2000-es évek második felében rohamosabb fejlődés volt tapasztalható az IT rendszerek minőségében, számában, funkcionalitásában, mint korábban. Minden az új és jobb felé mutat, azonban sok esetben ezek sem biztonsági fejlesztésekkel, sem jogi szabályozásokkal nem lettek megfelelően támogatva. Különböző folyamatok indultak el, amik az IT szektor szegmenseinek védelmében a fejlesztéseket célozták meg. Egyre jobban előtérbe került a biztonság, mind technikai, mind jogi oldalról. Ez a folyamat a piaci szegmensen és a nemzeti problémákon is túlmutatott. Ennek megoldására európai szintű szabályozásra volt szükség. Ezzel párhuzamosan a 2000-es évek pénzügyi válságai eredményeképpen 2010-től beindult a pénzügyi szektor szabályozása az operatív működés biztonságának szempontjából is. [1] Így más területek mellett, a bankszektor elektronikus pénz alapú fizetési módszereinek biztonságosabbá tétele is előtérbe került.

PÉNZFORGALMI SZABÁLYOZÁS

Az Európai Bizottság 2007-ben adta ki az *Európai Parlament és a Tanács 2007/64/EK irányelve (2007. november13.) a belső piaci pénzforgalmi szolgáltatásokról és a 97/7/EK, a 2002/65/EK, a 2005/60/EK és a 2006/48/EK irányelv módosításáról és a 97/5/EK irányelv hatályon kívül helyezéséről* szóló irányelvét (továbbiakban: PSD). [2] A fő célja az volt, hogy szabályozza az Európai Unió (továbbiakban: EU) és az Európai Gazdasági Térség (továbbiakban: EGT) területén a pénzforgalmi szolgáltatókat és szolgáltatásokat. Ezen belül az egyenlő piaci feltételek megteremtése volt a középpontban. A PSD biztosítja a jogi hátteret az Európai Fizetési Tanács (European Payments Council) – az európai bankszektor fizetési műveletekkel foglalkozó döntéshozó és koordinációs feladatokat ellátó testülete – által kidolgozott pénzfizetési megoldásokra, infrastruktúrákra és műszaki szabványokra vonatkozó harmonizációs törekvésére. A 2007. december 25-én elfogadott irányelveket 2009. november 1-jéig kellett harmonizálni az EU és az EGT tagállamainak a saját országuk jogrendjébe.

Az elmúlt közel 10 évben a korábban létező elektronikus fizetési módszerek mindegyike nagy fejlődésen ment keresztül, így különösen a fizetési célú mobilalkalmazások területe [3], valamint a korábban a dedikált adatkapcsolat helyett az internetet, illetve nyílt protokollokat használó fizetési megoldások. [4] A korábban elterjedt típusok mellé új megoldások, felületek kerültek piacra. Szükségessé vált tehát a PSD irányelv felülvizsgálata. A vizsgálat az Európai Bizottság javaslatára *Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változatának* 114. – a jogharmonizációról szóló – cikke tekintetében, az Európai Központi Bank és az Európai Gazdasági és Szociális Bizottság véleményezésével rendes jogalkotási eljárás keretében zajlott le. Az eljárás végén egy új irányelvet alkottak meg: *Az Európai Parlament és a Tanács (EU) 2015/2366 Irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről* (továbbiakban: PSD2). Ezt a tagállamok 2018. január 13-ától át kell ültetniük a saját jogi környezetükbe és alkalmazniuk kell az abban foglaltakat. [5; Preamb. 115.]

Az irányelv kapcsán több kérdés is felmerült. Valószínűleg csak a harmonizációs törekvések folyamán, illetve a bevezetést követően fog jobban kitisztulni a néhol talán túlszabályozott, néhol nagyon általános direktíva céljának megvalósíthatósága. Jelen tanulmány leginkább a Magyarország viszonylatában próbálja meg értelmezni a kérdéskört.

A VÁLTOZÁS SZÜKSÉGESSÉGÉNEK KÖRÜLMÉNYEI

A PSD2 létrejövetelének indokaként az irányelv sok okot sorol fel a preambulumban. Ezek közül kiemelendő az (1) bekezdés, mely szerint az EU-n belül „jelentős előrelépést sikerült elérni a lakossági pénzforgalom integrációja terén" [5; Preamb. 1]. A (3) bekezdés megfogalmazza, hogy szükség van az új irányelvre, mivel az 2007-ben elfogadott PSD hatálybalépése óta „jelentős technikai innováció zajlott le a lakossági pénzforgalmi piacon, gyorsan nőtt az elektronikus és mobilfizetések száma és a pénzforgalmi szolgáltatások új típusai jelentek meg". [5; Preamb. 3] Az európai egységes kártyás, internetes és mobilfizetés megteremtése, a nemzeti határok feloldása [5; Preamb. 4] nélkül nem valósítható meg, így célkitűzésként ez ismét belekerült az első pontok közé az irányelv létrejöttének okai között. Az irányelv számos célt határoz meg. Ezek közül technikai szempontból a következő bekezdésekben tárgyaltak fontosak.

Kiemelendő, hogy mind a jelenleg piacon lévő, mind a jövőben oda csatlakozni kívánó szereplők számára a folytonosság biztosítva legyen, illetve, hogy mindenki számára egy egyértelmű és harmonizált keretet nyújthasson, elkerülve bármilyen negatív megkülönböztetést a résztvevők között. [5; Preamb. 33] Fontos az, hogy nem csak a technológiák fejlődtek az elmúlt évtizedben, hanem a piacra új szereplők kerültek, akik nem voltak korábban integrálva a PSD által létrehozott rendszerbe. Az új változatban célként került meghatározásra, hogy minél szélesebb piacot érhessenek el az új fizetési megoldások. [5; Preamb. 6 és 27] Különösen igaz ez az internet alapú, hídként funkcionáló átutalásos jellegű banki platformokra, amelyek jellemzően fintech szolgáltatások.

A tagállamok a 2007/64/EK irányelv kivételekre vonatkozó részeit nagyon különbözőképpen értelmezték. Ez a fogyasztók kockázatának növelésén kívül a pénzforgalmi piacon történő verseny torzításához is vezetett. Az új irányelv tehát meghatározza, hogy a hatály alóli kivétel csak abban az esetben alkalmazható, ha az ügyfelek pénzeszközei nem kerülnek a pénzforgalmi közvetítőhöz és azok felett semmilyen befolyással sem rendelkeznek. [5; Preamb. 11] Erre a kitételre példák „az áruházi kártyák, az üzemanyagkártyák, a tagsági kártyák, a közlekedési kártyák, a parkolási kártyák, az étkezési jegyek illetve meghatározott szolgáltatási utalványok". [5; Preamb. 14] Kivételként határozza meg továbbá a kizárólag bankjegyek és pénzérmék fizikai szállításával foglalkozó pénzszállító és készpénzkezelő vállalkozásokat. [5; Preamb. 12]

Tisztázandónak tartja a jogszabály a különböző távközlési vagy más információtechnológiai eszközökkel történő fizetéseket, mivel ezek a legtöbb esetben hozzáadott értékkel is rendelkeznek. Szabályozandóak tehát a különböző mikrofizetési kategóriák közül többek között „a csevegésre, a letöltésekre, például videofilmek, zene és játékok letöltésére, a tájékoztatásra, például időjárás-jelentésre, hírekre, sporthírekre, tőzsdei hírekre és tudakozó szolgáltatásokra, valamint a részvételi televíziózásra, és rádiózásra, például szavazásra, vetélkedőkön való részvételre, élő visszajelzésekre vonatkozó szolgáltatások", illetve a különböző elektronikus jegyek és adományozáshoz kapcsolódó fizetési műveletek is. [5; Preamb. 15 és 16]

A kivételekkel történő visszaéléseket elősegítette az, hogy az eredeti irányelv nem kötötte hatósági bejelentéshez, ha egy vállalkozás ilyen szolgáltatásokat nyújtott. A PSD2 már kitér arra, hogy a releváns tevékenységekről az illetékes hatóságok meghatározzák, hogy valóban zártkörű hálózatok keretében működnek-e, mert csak ebben az esetben képeznek kivételt. [5; Preamb. 19]

A PSD2 GYAKORLATI ÁTTEKINTÉSE

Az Európai Unió egységes piacot célzó törekvései a PSD2 segítségével amellett, hogy a pénzmozgásokat azonnalivá szeretnék alakítani, többek között arra irányulnak, hogy a

bankkártya-társaságok egyeduralmából egy sokkal jobban megosztott piac jöjjön létre. Ez gazdasági szemszögből több ponton lehet érdekes. Sallai György rávilágít, hogy miért is alakulhat ki majd tisztább verseny a bankszektor ezen területén, ha más szereplők is jelen lesznek. [6]

Gazdasági szempontok

Eddig a bankkártyával történő fizetéskor nem közvetlenül a felhasználó bankjához kerültek a tranzakciók adatai, hanem a kártyatársaságok azonosítottak bennünket és a tranzakciót mind a két irányban. Ezért a szolgáltatásért a kereskedők voltak anyagilag terhelve, amely bevételből a bankok részesedést kaptak. Ezt az EU 2015/751 rendelete szabályozta, azonban ez nem volt elég. [7] A PSD2 segítségével a szolgáltatási piac megnyitása azonban eredményezheti a tisztább versenyt, melynek a végső nyertesei a felhasználók lehetnek.

Sallai rávilágít arra, hogy üzembiztonsági előnyökkel is jár a piac megnyitása. Példaként az Oroszország elleni szankciók bevezetését hozta, ahol a Visa és a MasterCard felfüggesztette a tranzakciós szolgáltatást, így gyakorlatilag súlyosan korlátozta a hétköznapok normális folyását. Ha csak néhány szolgáltató van a piacon és abból valamilyen okból néhány kiesik, könnyű belátni, hogy a tranzakciók nem fognak végbemenni. Azonban tekintsük meg az általános nyílt piaci viszonyokat. Ha több szolgáltatónak van lehetősége jelen lenni és abból néhány működésképtelen lesz valamilyen okból, akkor a többi még el tudja látni a feladatot. A szolgáltatás kiesés lehet egy fent említett szankció vagy akár egy rosszindulatú kód – például a napjainkban nagy figyelmet kapó ransomwarek egyike – aktivizálódása is.

A PSD2 oly módon nyitja majd ki, ezáltal feltehetően meg is változtatja az elektronikus fizetési piacot, hogy nem a megszokott kártyaadatokat megadási felülettel találja majd szemben a felhasználó magát. A majdani szolgáltató lesz az, akit meg kell adnunk egy fizetés során. Mindezek a műveletek egy teljesen egységes alapú webes felületen kellenek majd, hogy véghez menjenek.

Az elemzésből is kiderül, amit a téma kapcsán alapcélként tekinthetünk, hogy a fizetési lánc ily módon történő megváltoztatása elősegíti majd a résztvevők versengését a felhasználókért. Ezáltal egyre lejjebb szorítva a díjakat, egyúttal átláthatóbbá téve a piacon működő folyamatokat. Az áttekinthetőség az előírás szerinti, minden bankra kötelezően vonatkozó 20 elemű jegyzés elkészítésével válik teljesebbé. Egy összehasonlító oldalra kell a szabályozott pénzintézeteknek feltölteni a legjellemzőbb, díjköteles, fizetési számlához köthető szolgáltatásokat.

A direktíva meg fogja könnyíteni a bankváltás eddigi időbeni nehézségeit. Más kérdés, hogy Magyarországon az emberek többsége inkább aszerint választ bankot, hogy a lakhelyéhez melyiknek van közelebb bankfiókja, ATM-je. A könnyű váltás persze, mivel EU-s direktíváról beszélünk nem csak egy országon belüli bankváltást könnyíti meg. A rendelet célja, hogy feloldja azokat a korlátokat, melyeket a különböző tagállamok állítottak országhatáraikon belül. Így az adott szolgáltatók előtt nemzetközi lehetőségek nyílnak.

Ahhoz azonban, hogy a PSD2 keretrendszere a legjobban optimalizálható legyen, a társadalomnak fel kell ismernie a lehetőségeket az elektronikus fizetések kapcsán. Vannak olyan országok, mint például Japán, ahol az emberek többsége nem használ kézpénzt. Nem okoz tehát sem a fiatalkorúnak, sem az idős generációnak a kártyás fizetés. Itthon ez már kevésbé a valóság. Sokan ragaszkodnak a kézzel fogható fizetőeszközhöz. Ez itthon feltehetően az ország fejlődéséhez és a szocializációhoz vezethető vissza. Az EU törekvései a szürke-fekete gazdaság felszámolásával, az átláthatósággal pedig nyílván úgy valósítható meg, ha minél több pénzmozgásnak van látható nyoma.

Technikai megvalósítás

A 2018. elejében induló új fizetési lánc majdani résztvevői, feltehetően már elkezdtek készülődni, hogy a piac robbanásakor be tudják vezetni a saját megoldásaikat. A piaci nyitás törekvésének technikai oldalról vett alapja az úgynevezett banki API-k megnyitása [8]. Az API gyakorlatilag egy olyan modul, ami segítségével egy rendszer bizonyos részeit mások felhasználhatják saját felületükre. A legegyszerűbb példa, amikor a Google Maps API-ját használta, a Nintendo nagy sikerű Pokemon Go elnevezésű, a valóságot virtuális térré átalakító játéka. Itt a játék fejlesztői a megfelelő API-t használták, hogy rá tudják illeszteni a valós térképre a saját „világukat".

Valami hasonlót kell majd elképzelni a bankok kapcsán is. A pénzintézet köteles lesz biztosítani egy API-t, amihez a piacra lépő szolgáltatók (adott esetben maguk a bankok) a megfelelő engedélyekkel rendelkezve hozzáférhetnek az ügyfelek számlaadataihoz. Ehhez azonban az előírt engedélyekre van szükség, mind a kezdeti piacra jutási engedélyezési eljárás során megszerzett hatósági engedélyre, mind a felhasználó hozzájárulására az adott szolgáltatás igénybevételekor.

Szabályozás

Többek között Németh Monika is felveti a finteczone.hu-n [9] a túlszabályozottság kérdéskörét. A már korábban említett szolgáltatók rendszerbe történő beintegrálódásához szükséges előírások sok esetben nem kockázatarányosak. Emellett sok kritika éri az erős autentikációt szabályozni kívánó RTS (Regulatory Technical Standards on Strong Customer Authentication) előírást. Ahogy Németh is említi, a fő probléma az egyensúly megtalálása. Ez persze minden biztonsági rendszerben egy fontos alapkérdés. Feltehetően a kétfaktoros hitelesítés a kivételek megadásával manapság már nem annyira kényelmetlen. Így a félelmek talán csak a régebbi rossz gyakorlatból fakadnak.

Az tény, hogy az átlag felhasználó biztonságtudatosságának hiánya miatt plusz energiának tűnik egy második faktor beillesztése. Jelen technológia mellett, ahol a telekommunikációs cégek rendelkezésre állása, a hálózatok magyarországi lefedettsége egyre jobb, az SMS alapú második faktor beiktatása már nem lehet kényelmi hátrány. A biometrikus eszközök, tokenek is egyre szélesebb körben elterjedtek. Természetesen ezek plusz másodpercek, azonban optimista feltételezésünk szerint, egy ilyen mindenki által használt rendszer elindítása jó alkalom lesz a tudatosabb felhasználói szokások kialakítására.

Természetesen ez az intézkedés miatt az online fizetési felületek elveszíthetik a „one-click" típusú műveleteiket. De ne legyen kétségünk afelől, hogy azok a technológiai cégek, akik egy ilyen jövedelmező, új területből profitot szeretnének realizálni, azon lesznek, hogy a felhasználók minél egyszerűbben, kényelmesen tudják a szolgáltatásaikat igénybe venni. A sikerüknek ez lesz az egyik, hanem legfontosabb része, a megfelelő biztonsági előírások betartása mellet.

AZ ELEKTRONIKUS PÉNZFORGALMI SZOLGÁLTATÁSOK ELLENI HUMÁN ALAPÚ TÁMADÁSI LEHETŐSÉGEK

A social engineering, azaz az emberek céljaink érdekében történő irányítása, sok esetben összeforrt a hackelés fogalmával. [10] A támadás nem csak informatikai rendszerek ellen irányulhat. A banki, pénzügyi szektort fókuszba véve a támadás elsősorban adatok megszerzésére, illetve anyagi haszonszerzésre irányul. Megtörténhet, hogy valaki identitását használják saját célra a támadók, de az is előfordulhat, hogy olyan szolgáltatásokat hoznak létre, melyeknek a célja, hogy a gyanútlan áldozat pénzéhez jusson hozzá ellenszolgáltatás nélkül. Ebbe a kategóriába tartozik az olyan kecsegtető megoldás (pl.: mobil alkalmazás) nyújtása, mely elvégzi ugyan azt a funkciót, amiért az áldozat igénybe veszi (ingyen vagy fizetségért

cserébe), azonban a háttérben olyan is történik, melyet nem szeretne a szolgáltatást igénybevevő.

Mivel a nem szakmabeli emberek nem ismerik a lehetőségeiket, technikai tudásuk nem elegendő arra, hogy felismerjék a veszélyeket, így könnyen megvezethetőek. Ez különösen igaz a mobil eszközökkel kapcsolatos, illetve a közösségi médiában megjelent új készpénzkímélő megoldásokkal kapcsolatban. Az alkalmazáson belüli vásárlások, a hamis e-bank oldalak, a különböző online bankkártyák mind lehetőséget adnak a gyanútlan személyek kihasználására a különböző social engineering módszerekkel.

A magyar büntetőjog a készpénz-helyettesítő fizetési eszköz hamisítását és az azzal való visszaélést bünteti. Szerencsére az ilyen típusú bűncselekmények csökkenő tendenciát mutatnak. [11]

A VÉDELMI SZINT NÖVELÉSE A PSD2 SEGÍTSÉGÉVEL

A PSD2-ben leírt szabályozások alapvetően a pénzforgalmi szolgáltatást nyújtókra vonatkoztatott keretet határoz meg, mely mégis olyan következményekkel jár, ami a fogyasztók számára a biztonsági szint növelését segíti elő. Ezáltal közvetve hozzájárul a humán alapú támadások megakadályozásához, melynek alanya lehet a fogyasztó és a szolgáltatást nyújtó is. A legtágabb körű védelmi szint az, hogy az elektronikus pénzforgalmi szolgáltatást nyújtók csak engedélyhez kötötten végezhetnek ilyen jellegű tevékenységet, így ha nem felelnek meg a velük szemben támasztott követelményeknek, normál esetben nem is nyújthatnak ilyen szolgáltatásokat. Ahhoz, hogy egy pénzforgalmi intézmény működni tudjon, a székhely szerinti tagállam illetékes hatóságához kell fordulnia engedélyért.

Az ellen, hogy a szolgáltató lehetővé tegye a vevőtől történő pénz beszedését, de ellenszolgáltatást cserébe ne nyújtson az irányelv 7. cikke nyújt védelmet. Ez meghatározza, hogy a pénzforgalmi intézmények tőkéje – a szolgáltatások milyenségétől függően – nem csökkenhet 20 000, 50 000 vagy 125 000 EUR alá.

Az irányelv a személyes adatok védelmével, a különböző erre vonatkozó felelősség-meghatározásra irányuló jogi problémák megoldására is próbál megoldást találni. [5; Preamb. 29 és 30] A fogyasztó és a vállalkozó oldal különbsége miatt fontos megállapítani, hogy különböző szintű védelemre van szükségük, azonban jogállástól függetlenül az irányelvnek mindenkor alkalmazhatónak kell lennie. [5; Preamb. 53]

BANKKÁRTYÁS FIZETÉSI BIZTONSÁG A PCI DSS-SZEL

A PSD2 megnyitja a lehetőséget az alternatív készpénz-kímélő fizetési módok előtt, viszont ezek kevésbé szabályozott szolgáltatások, – ha nem is jogilag, mindinkább műszaki szempontból – mint a klasszikus bank- és hitelkártyás fizetési tranzakciók.

A szigorúbban szabályozott pénzügyi szolgáltatások előnye az, hogy pontosabban meghatározott biztonsági követelményeket írnak elő velük szemben. Jó példa erre a bankkártyás fizetési piac. Öt nagy bankkártya márka (American Express, Discover, JCB International, MasterCard és Visa Inc.) együttműködéséből született szervezet és bankkártyás fizetési biztonsági szabvány (Payment Card Industry Data Security Standard, PCI DSS) szabvány részletesen meghatározza a követendő biztonsági szabályokat. Így konkrétan előírja, hogy a bankkártyát elfogadó kereskedők illetve a bankkártyás fizetésben érintett szolgáltatók informatikai rendszereit hogyan kell kialakítani. A 139 oldalas szabvány – melynek legújabb 3.2.1 verziója 2018 májusában jelent meg – részletekbe menően meghatározza még azt is, hogy a tűzfal szabályok módosításairól milyen bizonyítékokkal kell rendelkeznie a szervezetnek. [12] A PCI DSS az informatikai biztonsági szabványok közül messze a legrészletesebb és lehető legpontosabban meghatározza a betartandó szabályokat. Ez persze nem teszi lehetetlenné

a visszaéléseket, – ahogy azokról a napi sajtóban is értesülhetünk – viszont jelentősen csökkenti az incidensek bekövetkezésének valószínűségét.

A PCI DSS minden olyan informatikai rendszerre és szervezetre vonatkozik, ahol bankkártya adatokat kezelnek, vagy pedig bankkártya adatok biztonság a múlik az adott szolgáltatáson. A szabványok vonatkoznak a rendszer infrastrukturális elemeire, az üzemeltető személyzetre, és a dokumentációkra is.

A szabvány első fejezete az informatikai hálózatok biztonsági követelményeit határozza meg. A biztonság legfontosabb meghatározó elemei a tűzfal és az útvonalválasztó (router). Az első fejezet nagy része ezek biztonságos konfigurációjáról, a konfiguráció központi tárolásáról. menedzsmentjéről és az új eszközökön az automatikus beállításáról szól.

A második fejezet az informatikai rendszerek és a hálózati infrastruktúra biztonságos konfigurációjával foglalkozik. Ezen belül az alapértelmezett jelszavak megváltoztatása, a hálózati konfiguráció védelme és a biztonságos alapbeállítások létrehozása a cél. Minden szervernek csak egy elsődleges funkciója lehet és csak a feltétlenül szükséges szolgáltatások futhatnak rajtuk. Minden, nem a konzol előtt végzett rendszergazdai műveletet csak titkosított csatornán lehet végezni.

A harmadik fejezet célja a tárolt hitelkártya adatok védelme. A legjobb az, hogyha elkerüljük az adatok tárolását, de ha erre nincsen lehetőség, akkor csak a legszükségesebb adatkört szabad kezelni, annyi ideig, ami elengedhetetlen az üzleti, vagy technikai cél eléréséhez és a titkos azonosító adatok (úgymint pinkód és a három számjegyből álló CVC2/CVV2 kód) kizárólag a kártyakibocsátók által tárolhatók. Azt, hogy ez minden esetben teljesül, kötelező a rendszerben vizsgálni. Véletlen tárolás lehet például a webszerver hibanaplójában. Alapvetően a bankkártyaszám megjelenítésénél maszkolásra kell törekedni, amikor csak az első hat és az utolsó négy számjegy jeleníthető meg legfeljebb. A tárolt adatokat titkosítani kell, ami történhet a táblázat, az állomány, vagy a teljes lemez titkosításával. A kulcsok kezelésének szabályait részletesen meg kell határozni, így például a szabadszöveges kulcsokat szét kell osztani.

A negyedik fejezetben a bankkártya adatok nyilvános hálózatban történő átküldése kerül szabályozásra. Alapvető követelmény itt, hogy csak megfelelő titkosítású protokoll használható. Az átlagosnál szigorúbb követelmény, hogy az SSL és korai TLS protokollokat a szabvány nem tekinti biztonságosnak. Ezek használata csak 2018 júliusáig lehetséges és akkor is csak megfelelő migrációs és kockázatcsökkentési terv mellett. [13]

Az ötödik fejezet a kártékony kódok elleni védelemről és az antivírus program naprakészen tartásáról szól. Előírás, hogy minden olyan rendszeren, ami ki van téve vírustámadás veszélyének, kötelező a vírusvédelmet biztosítani. A rendszeresen frissített és ütemezett teljes keresést végrehajtó víruskereső beállításaihoz csak az arra felhatalmazott felhasználói kör férhet hozzá.

A hatodik fejezet a biztonságos rendszerek fejlesztéséről és üzemben tartásáról szól. A különböző sérülékenységeket azonosítani és magas kockázat esetén három hónapon belül javítani szükséges. Ezzel előírva a rendszeres operációs rendszer és alkalmazás frissítések kötelezettségét. Szoftverfejlesztéskor külön feladat megfelelően biztonságos kód fejlesztése. Ezen belül a megfelelően kialakított változáskövetési rendszer, a szokásos programozási hibák és sérülékenységek kiküszöbölése, így különösen az OWASP TOP10 sérülékenységi lista kiküszöbölése.

A hetedik fejezet a bankkártya adatokhoz való hozzáférés korlátozásáról szól, amelynek meg kell felelnie az üzleti igényben meghatározott legkisebb tudás elvének. Elvárás, hogy erre külön hozzáférésvezérlési rendszer legyen létrehozva.

A nyolcadik fejezet a rendszerkomponensekhez való hozzáférések vezérléséről és azonosításáról szól. Szükséges a hozzáférések megadásának és menedzsmentjének a formalizálása. Ez történhet egy federált identitás menedzsment rendszer bevezetésével is akár, de alapvetően lokális gépen megfelelően szabályozott fiókok és hozzáférési engedélyek is

elégségesek. Ugyanígy külön foglalkozni kell a harmadik felek által a rendszerhez való hozzáférés korlátozásával. Szükséges a legalább hét karakteres komplex jelszó alkalmazása, amely legfeljebb három hónapig érvényes és nem egyezhet meg az előző négy jelszóval. A hat téves próbálkozást legalább harminc perces kizárás kell, hogy kövesse. A megnyitott kapcsolatokat tevékenység hiányában tizenöt perc után le kell zárni. A rendszergazdai hozzáférések esetében többfaktoros azonosítást kell alkalmazni. A csoportos, több felhasználó között megosztott, vagy az általános felhasználói fiókok használata tilos.

A kilencedik fejezet a bankkártya adatok fizikai hozzáférés-védelmével foglalkozik. Ennek keretében a szervertermet vagy az irodát kamerával meg kell figyelni, vagy kártyás beléptetőrendszerrel kell szabályozni a belépést. A hozzáférési adatokat vagy kamerafelvételt egy évig kell tárolni, ezen belül a legutóbbi három hónap adatainak azonnal visszakereshetőnek kell lenni. Ezzel kapcsolatban problémát jelent a személyi és vagyonvédelmi tevékenységet szabályozó törvényben meghatározott adattárolási idő. Amennyiben a PCI DSS által meghatározott követelmény valamely nemzeti jogi előírás miatt nem teljesíthető, akkor azt külön rögzíteni szükséges, de ilyenkor mindig a nemzeti jognak van elsőbbsége. A védett területen azonosítani kell és meg kell különböztetni a munkatársakat és a vendégeket. Ide tartozik a biztonsági mentések és minden más adathordozó fizikai védelme, a tárolás, a szállítás és a megsemmisítés kapcsán.

A következő fejezet a biztonsági naplózás előírásait határozza meg, így különösen a naplók tartalmát, a napi (sic!) logelemzés szükségességét és a naplók egy éves megőrzését egy dedikált naplószerveren vagy mentésekben. Itt foglalkozik a szabványalkotó az időszinkron beállításaival is, ugyanis ez is kiemelten fontos a naplók felhasználhatósága, valamint az azonosítás (authentikáció) esetében is.

A tizenegyedik fejezet a biztonsági tesztelés kérdéskörét tárgyalja, így az engedély nélküli vezeték nélküli hálózatok negyedévenként végzendő keresését, a külső és belső sérülékenység-vizsgálatokat szintén negyedévenként, az éves behatolási tesztelést (penetration test) és ugyanezt félévenként a hálózati szegmentációra vonatkozóan. A külső sérülékenység-vizsgálatokat csak a szintén PCI Council által meghatározott PCI Approved Scanning Vendor (ASV) programban részt vevő szervezetek végezhetnek.

Az utolsó fejezet a belső szabályzatokkal, adminisztratív kontrollokkal foglalkozik. Ezen belül az információbiztonsági politika és annak felülvizsgálata, munkavállalók biztonsági átvilágítása, képzések, beszállítók kiválasztása, felelősségek, hatáskörök tisztázása a szabályozott kérdések.

A fentiek alapján látható, hogy a PCI DSS meglehetősen részletesen szabályozza a bankkártyás fizetési biztonság területét, de alkalmazása viszont csak azokban az esetekben kötelező, ahol a fenti cégek bankkártyáival történik a fizetés. Így tehát minden olyan fizetési eljárás, ami kikerüli a legismertebb bankkártyákat mindennemű ellenőrzés nélkül működhet. Hasonlóképpen igaz ez az állami pénzmozgásokra. [15] Ezzel a kérdéssel viszont jelen cikkünkben nem foglalkozunk. A szerzők részéről talán nem alaptalanul merül fel az aggodalom, hogy a PSD2 bevezetésével az Európai Uniós pénzkímélő fizetési eszközök piacán hirtelen szabályozatlanul sokféle új fizetési mód jelenik meg. Ez nem jelenti azt, hogy ezek a fizetési módok rosszak lennének, viszont azok megfelelőségét nem kötelező vizsgálni és nincsenek is meg rá a megfelelő szabványok illetve a helyes iparági gyakorlat. Tehát az a szabályozás, ami a piacra lépést megkönnyíti könnyen sodorhatja veszélybe az állampolgárok anyagi biztonságát és egyben pénzügyi rendszerbe befektetett bizalmát. Ez utóbbi kiépítése több évtizedes komoly fejlesztés eredménye, beleértve azt is, amikor a bankok még az elvárhatónál is jobban igyekeznek kielégíteni az ügyfél biztonsági igényeit. Erre példa volt Magyarországon, hogy a MALÉV csődje esetében több bank visszatérítette a bankkártyával vásárolt repülőjegyet, amire pedig semmiféle kötelezettsége nem volt, kizárólag a bizalom erősítését szolgálta.

A fentiekkel szemben egy új típusú mobil fizetési eljárás sok esetben ismeretlen terület. A gyártó nyilván végez kockázat csökkentési lépéseket, de azoknak a pontos módjára nincsen jól bevált ipari gyakorlat, ami egyben azt is jelenti, hogy könnyen megeshet, hogy ezek a jónak tűnő védelmi intézkedések valójában nem megfelelően hatásosak és ezért incidensek történnek és a már kiadott szoftvert többször módosítani, rosszabb esetben visszavonni kell. A vevői bizalom másik kulcsfontosságú terület a hatékonyság és felhasználó barátság mellett, amely jellemző kihívása minden digitális szolgáltatásnak. Elég erre egy analóg példaként az elektronikus aláírást említeni, ahol húsz éve nem sikerült kialakítani azt a felhasználói bizalmat, ami a tömeges elterjedéshez szükséges. Így gyakorlatilag két évtized után is csak egyes részterületeken, különleges eljárásokban használják a digitális aláírást, pedig az az elektronikus hitelesség egyetlen valódi eszköze. Ennek legfőbb oka az, hogy a felhasználók nem értik a rendszer működését és így mint egy átláthatatlan matematikai eljárásra nem bízzák a szerződések hitelességét. Másrészről valószínűleg a használók nagy többsége a bankkártyás fizetési eszközök működését sem ismeri, de ott a praktikum és a széleskörű alkalmazhatóság, valamint az incidensek relatíve alacsony száma meggyőzte a használókat ennek a szükségességéről. Ez a bizalom az, amit egy rossz döntéssel, rossz termékkel, vagy egy szélesebb körű incidenssel nagyon gyorsan le lehet rombolni és elérjük vele, hogy a felhasználó visszatérjenek a készpénz alkalmazásához.

ÖSSZEGZÉS

A mindennapjainkat nagyban meghatározó különböző elektronikus tranzakciók védelme szerencsére egyre nagyobb figyelmet kap. Ez azért is fontos, mert a sűrűn használt bankkártyás fizetések mellett a piacon egyre jobban elterjednek a mobileszközökön történő mikrofizetések. Ennek a biztonságosabbá tételére a PSD2 jó védelmi megoldást nyújt mind az elektronikus fizetési megoldásokat szolgáltató, mind az ezeket igénybevevők számára. Az Nem szabad azonban a szakembereknek csupán azzal foglalkozniuk, hogy a jogharmonizáció után elérjék azt a szintet, hogy a PSD2-nek megfeleljenek. Törekedniük kell arra, hogy a lakosság figyelmét felhívják a saját naivitásukból, ismereteik hiányából fakadó olyan veszélyekre, melyek anyagi és erkölcsi károkat okozhatnak számukra. Ez, a védelmi megoldások beiktatása mellett, csak a megfelelő neveléssel, oktatással lehetséges.

FELHASZNÁLT IRODALOM

[1] KECSKÉS A.: *Európai jogi szabályozás és annak magyarországi implementációja a pénzügyi intézményeket érintő új kihívások területén*. In: TILK Péter (szerk.): Az uniós jog és a magyar jogrendszer viszonya. PTE, Pécs, 2016. Pp. 333-356.

[2] *Az Európai Parlament és a Tanács 2007/64/EK irányelve (2007. november 13.) a belső piaci pénzforgalmi szolgáltatásokról és a 97/7/EK, a 2002/65/EK, a 2005/60/EK és a 2006/48/EK irányelv módosításáról és a 97/5/EK irányelv hatályon kívül helyezéséről szóló irányelvét* (Payment Services Directive, PSD)

[3] Z. JORGENSEN, J. CHEN, C. S. GATES, N. Li, ROBERT W Proctor, TING Yu: Dimension of Risk in Mobile Applications; San Antonio, Texas, USA; 2015; ISBN: 978-1-4503-3191-3

[4] K. SUNG, J. KYU LEE: *Preference of Internet-based Debit Payment Protocols*; Liverpool, United Kingdom; 2011; ISBN: 978-1-4503-1428-2

[5] Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről, OJ L 337, 23.12.2015, p. 35–127 http://data.europa.eu/eli/dir/2015/2366/oj

[6] SALLAI Gy.: *Olyan változás jön, ami minden magyar bankkártyát érint;* http://www.portfolio.hu/vallalatok/it/olyan_valtozas_jon_ami_minden_magyar_bankkartyajat_erinti.229610.html (letöltve: 2018. 06. 01.)

[7] *Az Európai Parlament és a Tanács (EU) 2015/751 rendelete (2015. április 29.) a kártyaalapú fizetési műveletek bankközi jutalékairól, HL L 123.,* 2015.5.19., 1—15. o. http://data.europa.eu/eli/reg/2015/751/oj

[8] NYÁRY M.: *A banki adatok kötelező megnyitása: robbanás előtt a pénzügyi informatika* http://hirlevel.egov.hu/2016/11/21/a-banki-adatok-kotelezo-megnyitasa-robbanas-elott-a-penzugyi-informatika/; (letöltve: 2017. 03. 12.)

[9] NÉMETH M.: *Egy évvel a PSD2 után*; http://fintechzone.hu/egy-evvel-a-psd2-elfogadasa-utan/; (letöltve: 2017. 03. 12.)

[10] KOVÁCS L.: *Az információs terrorizmus eszköztára*, Hadmérnök, I. évf. 2006. különszám

[11] TÓTH D.: *A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények büntetőjogi szabályozása*. In: KECSKÉS Gábor (szerk.): Doktori műhelytanulmányok, Széchenyi István Egyetem, Győr, 2015. ISSN 2064-1788

[12] *Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures. Version 3.2.1* May 2018. PCI Security Standards Council, LLC.

[13] SZÁDECZKY Tamás: Kriptográfiai protokollok megfelelősége, Hadmérnök XI. évf. 4. sz. 2016. december. ISSN 1788-1919 pp. 178-183.

[14] SZÁDECZKY T.: *Information Security Law and Strategy in Hungar*y, Academic and Applied Research in Military and Public Management Science (ISSN: 2064-0021) 14: (4) pp. 281-289. (2015)

[15] SZABÓ ZS. M.: *A nyugdíjfolyósítás információbiztonsági és informatikai biztonsági kérdései,* In: Bitay Enikő (szerk.): A XXII. Fiatal Műszakiak Tudományos Ülésszak előadásai. Kolozsvár: Erdélyi Múzeum Egyesület (EME); Óbudai Egyetem, 2017. 4 p. (ISBN 978-963-449-018-0) pp. 363-366. (Műszaki Tudományos Közlemények - Papers on Technical Science)