

Banki levelező rendszer a felhőben

esettanulmány

Jakab Péter
vezető szaktanácsadó
MKB Bank Zrt.



A bevezetés

üzleti és operációs környezete

- Új üzleti stratégia
- Új IT stratégia
 - Az üzleti igényekhez történő gyors alkalmazkodás
 - Termék kiszolgálás
 - T2M lerövidítése
 - IT támogatott üzleti termék/szolgáltatás innováció
 - Szolgáltatás orientált IT
 - Költségek:
 - Kontrol
 - Csökkentés
 - Hosszú távú költség hatékonyság
 - Tervezhetőség



Az alkalmazás kiválasztás főbb szempontjai

- Jól körülhatárolható funkció
- A bevezetés mérsékelt kockázatú
- Vegyes üzem lehetőség
- „Probléma reprezentáns legyen” – jövőbeli fejlesztésekhez pilot szerep
- Gyors bevezetés lehetősége
- A levelező rendszer upgrade aktualitása (támogatás, funkcionalitás)



Jogi kockázatok



- Jogi környezet
 - A jog nem, vagy késve követi a technológiát
 - Bizonytalan, ellentmondásos értelmezésnek is teret adó környezet
 - PSZÁF körlevél
 - Hpt. - a „kiszervezés” követelményeinek való maradéktalan megfelelés
 - Szerződés kötés nehézségei
 - Bonyolult szerződés szerkezet
 - Értelmezési nehézségek
- Garanciák változásai a tanúsítványok irányába
- „Sopot Memorandum” (EU adatvédelmi biztosok kiadványa)
 - “A felhő technológia alkalmazása nem vezethet oda, hogy csökken az adatvédelem szintje a hagyományos adatkezeléshez viszonyítva”
- A jogalkotás ebben a pillanatban is folyik - Az európai adatvédelmi biztos véleménye „A számítási felhőben rejlő potenciál felszabadítása Európában” című bizottsági közleményről
- „Úttörő szerep” – referencia és tapasztalat hiány



A felhő alapú informatika kockázatai

- a) az adatvédelmi incidensek észrevétlenek maradnak
- b) adatokat továbbíthatnak nem biztonságos harmadik országokba
- c) az általános szerződési feltételek túl nagy mozgásteret biztosítanak a szolgáltatóknak, akik az adatokat saját hasznukra is felhasználják
- d) átláthatatlan az adatfeldolgozók láncolata, így az adatkezelő nem is tudja ki, hol, mikor végez adatkezelési műveletet az adatain
- e) az alvállalkozók összetett láncolata miatt a rendszerek auditálása lehetetlen
- f) az adatkezelő elveszti a kontrollt az adatai felett
- g) az adatkezelő nem tudja független harmadik féllel ellenőriztetni a rendszert
- h) az adatkezelő nem tudja az érintett jogait garantálni a szolgáltatónál

PSZÁF 4/2012. számú Vezetői körlevél és PSZÁF állásfoglalások

- „a szolgáltató adja meg az adatfeldolgozás lehetséges helyszíneit – ez a vonatkozó országok jogszabályi környezete miatt fontos, **lehetőleg kerülendő, hogy az EU-n, vagy a safe harbor-on kívüli helyre kerülhessenek adatok**”
- A HR tevékenység nem pénzügyi tevékenységet közvetlenül támogató aktivitás
 - „Amennyiben e tevékenység ügyféladatokat, s így banktitkot nem érint, akkor olyan ügyviteli tevékenységnek minősül, amelynél a kiszervezésnek a Hpt. 13/A. § (1)-(12) bekezdéseiben foglalt rendelkezéseit nem kell alkalmazni, egyéb esetben azonban a kiszervezés szabályai megfelelően alkalmazandók. „

Jogi háttér

EU Safe Harbor

16/1. kötet	[HU]	Az Európai Unió Hivatalos Lapja	119
32000D0520			
L 215/7		AZ EURÓPAI KÖZÖSSÉGEK HIVATALOS LAPJA	2000.8.25.

A BIZOTTSÁG HATÁROZATA

(2000. július 26.)

a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott „biztonságos kikötő” adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről

(az írtetés a C(2000) 2441. számú dokumentummal történt)

(EGT vonatkozású szöveg)

(2000/520/EK)

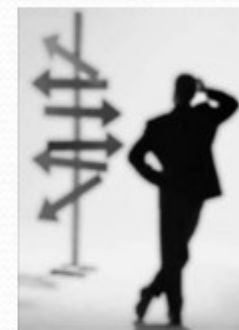
1. cikk

(1) A 95/46/EK irányelv 25. cikke (2) bekezdésének alkalmazásában, az Egyesült Államok Kereskedelmi Minisztériuma által 2000. július 21-én kiadott, e határozat II. mellékletében meghatározott gyakran felvetődő kérdések (a továbbiakban: GYFK) által biztosított útmutatással összhangban bevezetett, e határozat I. mellékletében meghatározott „biztonságos kikötő adatvédelmi elveket” (a továbbiakban: az elvek) az említett irányelv hatálya alá tartozó összes tevékenységre vonatkozóan úgy tekintik, mint amelyek biztosítják a Közösségből az Egyesült Államokban letelepedett szervezetek felé továbbított személyes adatok megfelelő szintű védelmét, tekintettel az Egyesült Államok Kereskedelmi

- Az EU általában tiltja az EGT-n kívüli adatfeldolgozók részére történő adattovábbítást, amennyiben az adott ország / vállalat nem biztosít megfelelő szintű védelmet, pl. "Safe Harbor" igazolással.
- Microsoft 2001. óta rendelkezik ezzel az évente megújított minősítéssel - <http://safeharbor.export.gov/companyinfo.aspx?id=19225>

Legfontosabb problémák

- Jogi kérdések
 - Adatvédelem – minden marad az EU-ban
 - On site visit jog
 - Alvállalkozókra vonatkozó követelmények – bevezetés alatt módosultak
- Technológiai kérdések
 - Public Folder
 - Mobil eszközök - hitelesítés
 - A „Big Bang” gyakorlatilag nem kivitelezhető



Legfontosabb problémák



- Migráció nehézségei:
 - Funkcionalitás (Public Folder)
 - Sáv szélesség igény a migrációnál
 - Korábbi Office verziók – direkt vs. közvetett upgrade
 - Korábbi archiváló rendszer kivezetése
 - AD adattisztítási igény – ami eddig nem volt probléma, az nem biztos hogy továbbra is probléma mentes

Tapasztalatok



- Limitációk pontos behatárolása, megértése
- Frissítések kezelése
- Licenzelési feltételek pontos tisztázása
- SLA pontos meghatározása és a szervezettel történő elfogadtatása
- HelpDesk alaposan felkészítendő

Tapasztalatok, kockázatok

- Végleges törölhetőség
- Titkosítási megoldások és problémák
 - Hol a kulcs, ki a valódi birtokosa?
 - Limitációk:
 - Alkalmazások oldaláról transzparens megoldás?
 - Performancia korlátok
 - Illetéktelen hozzáférés
 - Adatszivárgás
 - Key Management Interoperability Protocol (KMIP)
- BCM eljárások és korlátaik
 - Kapacitás problémák
 - Kritikus helyreállítási idők
- Az internet vagy más adatátviteli szolgáltatás megbízhatósága – nincs garancia, nem garantált szolgáltatás
- Hibakeresés – limitált lokális lehetőségek
- Az örök vita: Hol a hiba: szolgáltató?/internet?/lokális?
- Határidő csúszás – nem megy minden a „Nagy Könyv” szerint



A projekt főbb jellemzői

- 3000 postafiók
- 25 GB-os mail bokszt méretek
- 12 hónapos bevezetés több lépcsőben:
 - Előkészítés – jogi, technikai
 - Pilot üzem – kisebb kockázatú részterületekkel
 - Teljes átállás – szoros „post go live support”





Köszönöm a figyelmüket!