Vállalkozásfejlesztés a XXI. században 2022/1. kötet
Az üzleti szervezetek túlélési esélyei napjaink legújabb kihívásainak idején

Tudásmenedzsment és kiberbiztonság összefüggésrendszere a bankszektorban

Dr. habil. Szeghegyi Ágnes

Egyetemi docens, Óbudai Egyetem, Keleti Károly Gazdasági Kar
szeghegyi.agnes@kgk.uni-obuda.hu

Dr. habil. Kiss Gábor

Egyetemi docens, Óbudai Egyetem, Keleti Károly Gazdasági Kar
kiss.gabor@bgk.uni-obuda.hu

Gulyás Olivér

Phd hallgató, Óbudai Egyetem, Keleti Károly Gazdasági Kar
gulyaso@gmail.com

Absztrakt: A cikk célja a szervezeti tudásmenedzsment kiberbiztonságra gyakorolt pozitív hatásának igazolása a pénzügyi szektorban. A pénzforgalom és a pénzügyi szektor a gazdaság működésének egyik biztosítéka. A pénzforgalommal kapcsolatos problémák igen súlyos gazdasági és társadalmi gondokat okoznak. A pénzintézetek működésének elengedhetetlen feltétele az információ, a tudás folyamatos és megfelelő szintű áramlása. Tekintettel arra, hogy ezek a szervezetek szenzitív információkat, tudásokat kezelnek, és tárolnak, az információk védelme primordiális. Szekunder kutatási eredmények azt bizonyítják, hogy a hazai és nemzetközi vizsgálatok még mindig tárnak fel elemi biztonsági hiányosságokat. Ezeken a biztonsági hiányosságokon vagy réseken keresztül tudnak digitális vagy fizikai támadást indítani a hackerek. A támadások célja lehet a pénzintézeti szolgáltatások megakadályozása, az adatlopás, a vagyon eltulajdonítása. Magánszemélyek, idegen kormányok, a konkurencia egyaránt állhat ilyen támadások mögött. A cikkben továbbá egy konkrét példán keresztül, anonimizált módon vizsgáljuk meg egy pénzintézeti tudástár létrehozásával kapcsolatos problémakört.

Kulcsszavak: Tudásmenedzsment, tudásrendszer, tudástár, kibertámadás, kiberbiztonság, integrált informatikai rendszer, pénzügyi szektor

1 Bevezetés

A sikeresen működő szervezetek felismerték azt a tudásgyarapító képességet, amely a technológiában és az informatikában rejlik, másrészt azt a tényt, hogy az ezekben rejlő lehetőség csak akkor ér valamit, ha pontosan tudják, miből áll össze és hogyan osztódik szét a tudás. A tudás a szervezetek működésében betöltött szerepének megértése, a szervezet intellektuális tőkéjének hatékony felhasználása és fejlesztése az adott gazdasági szereplő tartósan sikeres működésének kulcsa. A tudás értékének és szerepének fokozatos növekedésével már az ezredforduló fejlődő iparága a tudásgazdálkodás lett, azaz tudással kapcsolatos tevékenységek elméleti hátterének, gyakorlatának és eszközrendszerének kialakítása. A tudásgazdálkodás, a tudásmenedzsment célja a minél nagyobb szervezeti tudáskombináció létrehozása, és folyamatos növekedésének biztosítása. Ennek előfeltétele a tudásmenedzsment funkcionális elemeinek, a tudáspiacnak, tudásteremtésnek, tudásrendszernek és tudástranszfernek integrált működése. A kihívás ma már nem az információhoz történő hozzáférés, hanem a rendelkezésre álló adatok, információk és tudás hatékony feltérképezése, felhasználása, egymással történő megosztása. Ez a tény a különböző szakterületeken működő szervezeteken, intézményeken belül felhalmozott ismeretanyagra is érvényes, és az azokkal történő gazdálkodásra. Adott szakterületen jelen lévő gazdasági szereplők pozíciójának, piaci értékének, versenyképességének megítélésében meghatározó szerepet játszik, hogy milyen mértékben képesek egy tudás megosztásán alapuló közösség aktív tagjaiként működni. A cikkben a tudásmenedzsment specifikumait vizsgáltuk a pénzintézetek működésének vonatkozásában.

A bankok jelentős volumenű információval dolgoznak, ezeket összegyűjtik, tárolják, feldolgozzák, és működésük elengedhetetlen feltétele ezek transzferálása is. Tekintettel a bankok által kezelt információk bizalmas, alkalomadtán titkos jellegére, a pénzügyi szervezetek működése szempontjából meghatározó tényező az információk, a tudás védelme. A cikkben ezért elemezzük az információbiztonsággal kapcsolatos legjelentősebb kihívásokat is.

Végül összegezzük egy konkrét szervezet tudástárának létrehozásával kapcsolatos tapasztalatokat, valamint egy integrált informatikai fejlesztés bevezetésén keresztül vizsgáljuk meg egy adott pénzintézet tudásbázisának optimális externalizálását. Ebben a fejezetben kitérünk egy integrált tudásbázis létrehozásának elengedhetetlen feltételét képező, megfelelő projektmenedzsment technikák alkalmazására.

A szükséges információk, tudás eljuttatása a megfelelő helyre már önmagában is kihívás egy nagyobb szervezetben. A pénzügyi szektor sajátossága az információk, a tudás fokozott védelme mind annak tárolásakor, mind pedig annak továbbítása közben, és máris megérkeztünk kutatásunk céljához: Tudásmenedzsment és kiberbiztonság a bankszektorban.

1.1 Tudásmenedzsment működése a pénzintézeteknél

A tudással történő eredményes és hatékony gazdálkodás ma már nem lehetőség, hanem üzleti kényszer. Egy szervezet sikereinek meghatározó tényezője tudástőkéjének hatékony felhasználása és fejlesztése. A tudástőke elemei:

- a kapcsolati tőke, mely a külső struktúrákat jelenti, a piaci szereplőkkel kialakított kapcsolatot,
- a szervezeti tőke, mely a belső struktúrákat jelenti, a szervezet korábbi működésének eredménye,
- a humán tőke, mely a dolgozók tudását jelenti, képességet tárgyi és eszmei vagyon létrehozására.

Egy szervezet tudástőkéjével kapcsolatos megválaszolandó kérdések:

- Tudja-e a vállalat, hogy milyen tudást birtokol?
- Megoldott-e a tudás rendszerezése?
- Csak releváns információkat gyűjt-e a vállalat?
- Egy kolléga távozásával megmarad a volt kolléga tudása?
- Tacit tudás mindenki számára érthetően megfogalmazásra került? (Skoll, 2021)

1.1.1 Szervezeti tudástőke létrehozása

A szervezetfejlesztés egyik kulcseleme a tudásmenedzsment funkcionális elemeinek kialakítása, integrált működésük biztosítása. A tudásmenedzsment napjainkban az egyik domináns kutatási terület, amely a szervezeti tudással kapcsolatos tevékenységekkel foglalkozik. Azaz az egyéni tudások megszerzésével, szervezeti tudás feltérképezésével, a szervezeti tudás felhasználásával, gyarapításával, felhalmozásával, a tudásbázis integrálásával, szinergikus hatások tudatos gerjesztésével, a szervezeti tudás tervszerű megosztásával, új értékek előállításával.

Fontos kiemelnünk, hogy a tudástár létrehozása már önmagában is sok kihívást jelent egy szervezet számára. Amennyiben a tudáspiaci mechanizmus, tudásteremtés folyamata, a tudásrendszer és tudástranszfer nem működnek kellő hatékonysággal, a tudástár megalkotása is komoly akadályokba ütközik.

A tudástőke létrehozásánál kiemelten fontos szempont, hogy a szervezet minden tagja érdekelt legyen a tudásgyűjtés folyamatában.

Minden szervezetnek törekednie kell arra, hogy a számára legfontosabb információkat összegyűjtse és értelmezze, azokat saját előnyére fordítsa azáltal, hogy tudást képezzen az adat - információ - tudás - bölcsesség hierarchiájának megfelelően. (Wapenaar J., 2022)

Egy vállalatnál a tudásmenedzsment bevezetése csak akkor válhat sikertörténetté, ha változtatunk a prioritásokon. (Ellie, O, 2018)

1.1.2 Szervezeti tudástőke fejlesztése

A tudástőke egyszeri létrehozása nem egy befejezett történet. Folyamatosan fel kell tárni az új információkat, tudásokat, ezekkel ki kell egészíteni a meglevőket, vagy felül kell írni azokat. Felülírás esetében fontos problémakör a régi információk tárolása, archiválása.

Néha a módosított adatok és/vagy az adatok módosítása is információt hordoz. Bizonyos visszaéléseket pont akkor tudnak a bankok észlelni, amikor a cégek egyes adatait módosítják. Az adatok módosítása úgynevezett korai figyelmeztető jelként előre jelezhet csalárd tevékenységet. Nem jelenti azt, hogy biztosan visszaélés történt, vagy fog történni, de fennáll a veszélye. A belső szabályzatok alapján meg kell vizsgálnia az üzletkötőnek az adott helyzetet!

1.1.3 Szervezeti tudástőke megosztása és felhasználása

Egy vállalat eszközei, forrásai korlátozott értékűek mindaddig, amíg a vállalat dolgozói nem tudják jó hatásfokkal alkalmazni, felhasználni azokat. (Girard, John P.; Girard, JoAnn L, 2015)

A szervezeti tudástér megosztásának szükségességét könnyen beláthatjuk. Az ismeretek rögzítése nemcsak egy adott helyzet, ügyfél bejelentés stb… megoldásában segít, hanem a későbbiekben, más ügyfélnél is, akinél ugyanez a kérdés merül fel. (Holsapple, C., 2003)

A tudásmenedzsmenten belül a tudástőke megosztása egy folyamat, mely rendszeresen, egyre gazdaságosabban és gyorsabban, szinte automatikusan listázza a felgyülemlett tudást, és határozza meg a lépéseit annak, ahogy a tudás megosztásának meg kell történnie! (Davenport, T., 2013)

A szervezeti tudástér létrehozása annak megosztása nélkül nem létezhet. Ezt axiómának gondolhatjuk a legtöbb szervezet működésénél. Azonban fontos kiemelnünk, hogy a pénzintézetek működésénél bizonyos esetekben csak az információk tárolása a jogszabályi vagy rendeleti elvárás.

Például a hitel dokumentációk esetében nem az adatok megosztása a fő szempont, hanem az, hogy a hitelkérelem vagy a döntési pontok megfelelően rögzítésre kerüljenek! De ugyanez igaz például bizonyos folyósítási feltételek esetében is. A benyújtott információk tárolása és archiválása jogszabályi előírás, az azonban már nem elvárás, hogy az információk visszakereshetők, megoszthatók legyenek.

Egy szervezet elemi érdeke, hogy az adatok és/vagy a dokumentumok ne csak rögzítésre kerüljenek, hanem – hacsak ez technikailag nem ütközik akadályba – visszakereshetők is legyenek! Ha technikailag nem biztosítható az adatok

katalogizálása, azaz tudáskatalógus és tudástérkép létrehozása, akkor előfordulhat, hogy csak a minimumfeltételek teljesítése, az archiválás a cél.

A létrejövő tudásbázisok nemcsak kezelni hivatottak az ismereteket, hanem tematikus keretek közé szorítva teszik elérhetővé azokat egy közösség számára. (Nonaka, I., von Krogh, G., 2009)

A megosztás fontos ismérve, hogy az információk, tudás összegyűjtését követően biztosítva legyen a hozzáférés a dolgozók számára. Az egész szervezet eredményességére negatív hatást gyakorol, ha az információkhoz, tudáshoz való hozzáférés nehézségekbe ütközik a belső kommunikációs csatornákon. A megosztásnál a hozzáférés biztosítása, a megfelelő jogosultságok meghatározása és a kommunikációs csatornák működése meghatározó szempont.

Megosztásnál fontos paraméter az idő is. A munkához szükséges adatok, információk, tudás letöltésének időigénye sokszor kritikus pont. Összetett információs rendszerek esetében az adatok kinyerésének bonyolultsága okozhat problémát. Az adat megtalálása, később például a szükséges dokumentum letöltése kulcskérdés.

Amennyiben egy adott dokumentumot nem, vagy csak nagyon nehezen találnak meg a dolgozók, akkor előbb-utóbb megtalálják a módját annak, hogy kerülő úton jussanak a számukra szükséges információkhoz, tudáshoz. Amikor nem a folyamatosan frissülő online tudásbázisokból töltik le a releváns információkat, hanem egymásnak küldözgetik az általuk jónak gondolt dokumentumokat, például nyomtatványokat, akkor könnyen előfordulhat, hogy már nem az aktuális verziót használják, hanem egy sokkal korábbit. Ezáltal az adott folyamat végén plusz munkát generálnak, és összességében többlet erőforrást kötnek le a szervezet egy másik területén.

A tudástőke megosztásának problémaköre leginkább az új belépőknél csúcsosodik ki, mert ők azok, akik nem rendelkeznek információval, tudással a szervezet belső ügyeiről. Azonban az új kollégák esetében a tudáshiányuk miatt könnyebb velük megértetni, és elfogadtatni egy bonyolultabb tudásbázis vagy nyilvántartó rendszer kezelését. Mivel számukra a kezdetektől természetessé válik a szervezeti tudásrendszer fizikai eszköze, a kollektív tudást tároló rendszerek használata, nem fogják a régi, korábban letöltött dokumentumokat használni, ezért kénytelenek mindig újonnan letölteni azokat. Visszatérve az információk védelméhez, ezért kerül biztosításra, hogy egyrészt nem tárolnak a saját gépükön információkat, másrészt mindig az aktuális információkat töltik le.

1.1.4 Vállalati tudástőke a pénzintézeteknél

Az információkhoz való hozzáférés megkerülhetetlen kérdésköre a pénzintézetek működésének. Általános megközelítés, hogy mindenki csak a számára szükséges információhoz jusson hozzá. Ez néhány konkrét példán keresztül:

- A vállalati ügyfelekkel foglalkozó üzletkötők esetében szükséges-e lakossági ügyfelek adatait látni?
- A lakossági ügyfélkezeléssel foglalkozók esetében mennyiben szükséges a vállalati ügyfelek adatait látni?
- Lakossági ügyfelekkel foglalkozó dolgozók esetében a saját kollégájuk, ad absurdum vezetőjük lakossági hitelét is láthatják?
- Lakossági ügyfelekkel foglalkozó dolgozók minden lakossági ügyfél adatát láthatják?
- Amennyiben a pénzintézetnél vezeti a számláját egy híres ember, egy politikus, akkor az ő számláját is láthatja bárki, aki lakossági ügyfelekkel foglalkozik?
- Vállalati ügyfelek esetében a kérdés ugyanaz, mint lakossági ügyfeleknél:
  - Minden vállalati ügyfél adatait láthatja minden vállalati üzletkötő?
  - Mi a helyzet a tőzsdei cégekkel?

A hozzáférési jogosultságok meghatározásán kívül fontos szempont, hogy minél egyszerűbb módon férjenek hozzá a dolgozók az információhoz. A tudás megfelelő szintű kodifikációján kívül legalább annyira fontos azok megfelelő publikációja.

A szervezeti tudástár létrehozásakor az ismétlődő bejelentések már sokkal kevesebb időt vesznek igénybe. A teljeskörű tudásbázis létrehozásával a tapasztalatok szerint az ismétlődő bejelentések kezelésének időszükséglete akár 20%-kal is csökkenhet. (Prónay G., 2013)

A gyorsabb kereshetőség erőforrást szabadít fel, és nagyban növeli mind az ügyfél, mind az alkalmazott elégedettségét.

A legtöbb vállalatnál a tudásmegosztás e-mail formájában történik. A levelek archiválhatók, visszakereshetők. Belső alcsoportokat alkotva könnyen el lehet juttatni az információkat egy adott csoport tagjaihoz. Pénzintézetek esetében azonban az e-mail-es tudásmegosztás nem elegendő. Az archiválás érdekében legtöbbször az adatokat különböző rendszerekbe is fel kell tölteni! Onnantól kezdve, hogy a szervezetek, jelen esetben pénzintézetek, a működésük során használt adatokat, információkat, tudást elkezdik nagy mennyiségben tárolni, az állandó hozzáférés mellett a folyamatos védelem is megoldandó probléma.

A közös szervezeti tudásbázis használata nemcsak az aktuális információk, tudás fenntartása miatt érdekes, hanem amiatt is, hogy egy központi regisztert fenntartani és megvédeni sokkal egyszerűbb, mint a felhasználók saját gépén tárolt információk védelmét biztosítani.

2 Információbiztonság és kibervédelem

2.1 Kibertámadások

A kibertámadás megnevezés alatt kell érteni minden olyan műveletet, melyet számítógépek, számítógépes rendszerek ellen indítanak. Egy-egy ilyen művelet az adatlopást, az informatikai rendszer elérhetetlenségét, de akár teljes tönkretételét is célozhatja. Minél magasabb jogosultságot sikerül szereznie a támadónak a megtámadott rendszerben, annál szélesebb körű a károkozási lehetőség. (Rohmeyer, Paul; Bayuk, Jennifer L, 2019)

2020-ban egy meghallgatáson Jerome Powell, a Federal Reserve elnöke a kibertámadásokat jelölte meg, mint olyan veszélyforrást, mely komoly aggodalmat kelt. A beszédében kiemelte, hogy a tradicionális veszélyekre, mint a rossz hitelek vagy hasonlóak, fel vannak készülve. Azonban a kibertámadások adnak aggodalomra okot. (Fred Imbert, Jeff Cox, Pippa Stevens, 2020)

A pénzintézetek adatait és információit tároló számítógépes rendszerekbe való engedély nélküli behatolás majdnem minden országban bűncselekmény. A digitalizációval, az informatika vagy az Internet fejlődésével megszűntek a földrajzi korlátok. A hacker támadások sem maradnak országhatárokon belül. Nem ritkák az olyan esetek, amikor a támadó az egyik ország joghatósága alá tartozik, míg a megtámadott esetében más állam az illetékes. A felderítés igazi nehézsége akkor kezdődik, amikor a támadó mögött az adott ország kormánya áll. A kormányzati inspirációra elkövetett cselekmények tetteseit, ha meg is találják, akkor sem vonják felelősségre. A pénzintézetek gazdaságban betöltött szerepüknél fogva akár ilyen, kormányzatilag szervezett behatolások célpontjai is lehetnek. (Evans, Lester, 2020)

A kezdeti, nem igazán válogatós vírus - (féreg) támadások mellett a célzott, egyedi felhasználókra irányuló offenzívák is megjelentek. Közvetlen támadási célok lehetnek az online vagy offline identitáslopás, személyes és üzleti adatok ellopása, a bankkártyák és bankszámlák adatainak eltulajdonítása, illetéktelen behatolás az online felhasználói fiókokba. Bár a fenti módok is komoly károkat okoznak, de súlyosabbak azok a támadások, amelyek célja maga a pénzügyi rendszer megbénítása. (Rohmeyer, Paul; Bayuk, Jennifer L., 2019)

A sok millió dolláros/eurós anyagi veszteség mellett a kibertámadások egyéb károkat is okoznak. A legfontosabb talán az ügyfél bizalmának ideiglenes vagy végleges elvesztése. A különböző technikákkal kivitelezett támadások mára már mindennaposakká váltak, ezért a megfelelő színvonalú védelmi intézkedések mellett a vállalat minden dolgozójának éberségére szükség van. A professzionális szinten kivitelezett támadások szükségessé teszik az érintettek közötti együttműködés javítását. A várható haszon nagysága miatt megéri, hogy a

pénzintézetek elleni támadásokhoz komoly és időigényes előkészületeket tegyenek. (BaFin, 2020)

2.2 Kritikus infrastruktúrák

A pénzügyi rendszerek a gazdaságban betöltött szerepük miatt nemcsak a szó átvitt, de tisztán jogi értelmében is kritikus infrastruktúrák. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény egyértelműen nevesíti azokat az úgynevezett létfontosságú rendszerelemeket, melyek adott ágazatokba tartozó szolgáltatások esetén elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához. A törvény alapján az 1. mellékletben meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához. A listán belül kiemelt az egészségügy, a lakosság személy- és vagyonbiztonsága, a gazdasági és szociális közszolgáltatások biztosítása, az ország honvédelme. A jogszabály szövege szerint ezek kiesése a feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.

2012. évi CLXVI. törvény 1. sz melléklete kifejezetten nevesíti:

- 20. Pénzügy pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei,
- 21. bank- és hitelintézeti biztonság,
- 22. készpénzellátás.

Tekintettel arra, hogy a 2012. évi CLXVI. törvény 2. § 9) pontja alapján a honvédelmi rendszerek és létesítmények ágazati kijelölő hatósága az 1. mellékletben meghatározott, nem honvédelmi ágazatba tartozó rendszerelemet honvédelmi érdekből, kormányrendeletben meghatározott honvédelmi kritériumok alapján, horizontális kritériumok vizsgálata nélkül nemzeti létfontosságú rendszerelemmé (a továbbiakban: ágazaton kívüli honvédelmi rendszerelem) kijelölheti. Az előzőek alapján a bankok működése a kritikus infrastruktúra alá tartozik. A pénzintézetek átfogó szabályozása már emiatt is elengedhetetlen.

2.3 Biztonsági helyzet

A 2021-es év első felétől kezdve a pénzintézeteket érintő internetes csalások csaknem megduplázódtak. A Which? a brit pénzintézetek biztonságát értékelte. Vizsgálták, hogy milyen erősségű védelmet adnak a bankok által használt bejelentkezési és fiókkezelési, titkosítási, a védelmi eljárások.

Bár a felhasználók valódiságának ellenőrzésekor már többlépcsős azonosítást alkalmaznak a bankok, az elvégzett biztonsági vizsgálatok több hiányosságot is feltártak. A felmérés során találtak olyan bankot, amely egyetlen számsort is

elfogadott jelszóként, de az olyan bonyolultságú jelszavak, mint az „admin" megadása is lehetséges volt. Más esetekben olyan jelszavakat is engedélyeztek, amelyek család- vagy keresztnevek is lehettek. A felmérés idején egyes bankok még mindig SMS alapú beléptetési rendszert használtak, amiről már régóta mondják a szakértők, hogy viszonylag könnyen kijátszható. A vizsgálat kiemelte, hogy bizonyos esetekben az al-domain védelmével volt probléma. Amennyiben ezeknek a védelme nem megfelelő, a támadók könnyen hozzáférhetnek akár a szerverekhez is. A vizsgálatok során olyan oldalt is találtak, ahol hiányoztak a felhasználókat, például belépéskor figyelmeztető biztonsági üzenetek. (Portfolio.hu, 2022)

A fenti kutatás kiemelte, hogy bizonyos esetekben még a megfelelő szűrőszoftverek sem álltak a bankok rendelkezésére. A szűrő szoftverek emberi beavatkozás nélkül már olyan feladatok ellátására is alkalmazhatóak, mint az álcázott üzenetek kiszűrése, karanténba helyezése, blokkolása. Igencsak kockázatos az a tény is, hogy találtak olyan pénzintézet, melynek oldala az első netbanki bejelentkezés után nem kéri többet a felhasználót, hogy adja meg a jelszavát. (Portfolio.hu, 2022)

A hazai pénzintézeti informatikai támogatással kapcsolatos felmérések alapján a legnagyobb kockázatot még mindig az elavult támogató rendszerek használata jelenti. A probléma felszámolását nehezíti az, hogy az elöregedett szoftverek lecserélése sok időt, pénzt, valamint rengeteg belső és külső erőforrást igényel. Figyelembe véve az aktuális munkapiaci trendeket, szakmailag felkészült és tapasztalt fejlesztői és projekt menedzseri erőforrást találni, és azt megfizetni komoly kihívást jelent bármelyik szervezetnek. Az erőforrások szűkössége miatt a korábban már felismert sebezhetőségek kezelésével kapcsolatos intézkedések is sokszor elmaradnak, ezzel tovább javítva a potenciális támadók esélyeit. Sajnos még mindig nehéz elmagyarázni a pénzügyi döntéshozóknak, hogy miért költsenek jelentős összegeket olyan biztonsági megoldásokra, amelyeket remélhetőleg soha nem fognak használni.

Az ügyfélbizalom szempontjából fontos üzletmenet folytonosság tervezésében és konkrét kivitelezésében is tapasztaltak hiányosságokat. Amikor egyszerre történnek a pénzintézet informatikai rendszerében a kritikus események, például valamilyen fizikai kár és egy online betörés, mivel nincsenek meg a megfelelő, közismert eljárások a problémák kezelésére, könnyen az informatikai támogatást használók fejére omolhat minden. (Mihály, Z., 2021)

Viszonylag új típusú kockázat a felhő alapú informatikai szolgáltatások sérülékenysége. A hazai pénzintézetek meglehetősen megfontoltan nyitnak a felhő alapú szolgáltatások használata felé. A pénzintézetek a felhőbe általában nem a kritikus fontosságú, az ügyfelek számláit vezető alaprendszereket, úgynevezett *core* rendszereket viszik. A jelenlegi informatikai trendek szerint a nagy adatkezelési kapacitásokat igénylő funkciók támogatását szervezik ki külső

szolgáltatókhoz, mint a levelezés, a videókonferencia megoldások vagy a csalásmegelőzés.

A pénzügyi szervezetek az informatikai rendszerek fejlődésével kapcsolatos trendek ismeretében arra számíthatnak, hogy egyre több sebezhető pont alakul ki az általuk használt informatikai rendszerekben. Az új sebezhetőségi pontok megjelenése természetszerűleg a támadók dolgát teszi a korábbiaknál még könnyebbé. A fentiek miatt a pénzügyi szektor informatikai rendszereivel szemben a kibertámadások száma előre láthatólag tovább fog növekedni. (Mihály, Z., 2021)

3 Integrált informatikai fejlesztés keretében vállalati tudástár létrehozása

A tudásmenedzsment részfolyamata:

- az információs hézagok feltérképezése,
- adat, információ és tudásgyűjtés a kollégák bevonásával,
- tacit tudás explicitté alakítása,
- kommunikációs csatornák kiépítése,
- a tudásmegosztás szervezeti kultúra szintjén való elterjesztése. (Yates P., 2022)

A tudásmenedzsment átfogó témáján belül a tudásgazdálkodás az a terület, amelynek célja kifejezetten a tudással kapcsolatos tevékenységek elméleti hátterének, gyakorlatának és eszközrendszerének kialakítása. Ahogy korábban már tárgyaltuk, a legnehezebb nem is az információkhoz, tudáshoz való hozzáférés, hanem a rendelkezésre álló adatok, információk, tudás feltérképezése, elérhetőségének biztosítása, hatékony felhasználása és megosztása. A létrehozott kollektív tudás rendszerezése, megosztása egy komplex szervezeten, jelen esetben egy pénzintézeten belül a szükséges informatikai háttér nélkül napjainkban már megvalósíthatatlan. (Skala, K., Davidović, D., Afgan, E., Sović, I. &; Šojat, Z., 2015)

A fentiekhez eszközökre és/vagy szoftverekre van szükség. Az önálló szoftverektől a bonyolult vállalatirányítási rendszerekig széles a skála a felhasználható technológiákban. (Anthony J., R, 2022) .Tudásmenedzsment gyakorlati működését legjobban egy konkrét példán keresztül mutatjuk be.

A cikkben egy integrált informatikai fejlesztés bevezetésén keresztül vizsgáljuk meg egy pénzintézeti tudástár létrehozásának legfontosabb kérdéseit.

3.1 Integrált informatikai fejlesztés

Összetettebb pénzügyi szervezeteknél a szervezet stratégiája, célkitűzései, feladatai, valamint szervezeti felépítése teszik szükségessé a feladatellátás folyamatában szereplő és támogató / megvalósító informatikai környezet létrehozását.

Pénzintézetek intézményi céljai között szerepel a naprakész tudásbázis létrehozása. Ennek keretében a kitűzött cél a makroprudenciális, a mikroprudenciális, valamint a fogyasztóvédelmi tevékenység hatékony megvalósításának biztosítása, továbbá a felhalmozott tudás megosztása, amelyet maximális mértékben egy integrált működést támogató eszköz használatával lehetséges megvalósítani.

A fenti célokat szem előtt tartva elvárás egy olyan integrált rendszer kialakítása, amely biztosítja:

- a folyamatok vezérlését és átláthatóságát,
- a határidők betartatását,
- a vezetői kontroll megvalósítását,
- a folyamatok teljes körű dokumentáltságát,
- megkönnyíti a mindennapi munkavégzést,
- lehetővé teszi a tevékenységek monitorozását, statisztikák előállítását,
- a vezetői információs igény kiszolgálását. (Bunkóczi L., Pető I., Pásztor M. Zs, Popovics A., 2015; Richard S., Jane N., 2020)

Az integrált informatikai fejlesztések esetében egy jó rendszer integrálja a jelenleg szigetalkalmazásként működő rendszereket, egyfajta hídfunkciót ellátva közöttük. (A Microsoft Dynamics 365 Business Central , 2022) Emellett a folyamatok, a jogosultságok ebben a rendszerben kerülnek definiálásra. Valamint a rendszernek képesnek kell lennie a dokumentumsablonok generálására, előre rögzített attribútumok automatikus kitöltésére, iktatására, statisztikai adatok előállítására rögzített paraméterek kiválasztásával. Segítségével a nyomon követhető információáramlás is biztosítottá válik. (Leah C., 2022)

Fontos, hogy a tevékenységgel kapcsolatos igények több irányból merülnek fel. Egyrészt a tevékenység folyamat alapú támogatása, illetve a kezelt ügyfelek komplex kezelése, másrészt a vezetői információs igény felől. (https://www.acterra.hu/vallalatiranyitasi-rendszer, 2022)

Integrált informatikai fejlesztés keretében vállalati tudástár megvalósításának előnyeit összefoglalva:

- Az igények megvalósítása esetén a folyamatok, a döntési pontok informatikai rendszerben rögzítettek és nyomon követhetőek.

- A folyamatokat csak a megfelelő jogosultsági szinten lévők végezhetik, és minden esetben a jóváhagyások - ki, mikor és mit hagyott jóvá - is rögzítésre kerülnek. (vallalatiranyitasi-rendszer.hu, 2022)
- A jogosultságkezelés megvalósításával és a nem zárt rendszerek - például Excel - használatának minimalizálásával biztosíthatóvá válik az adatbiztonság, adatvédelem.
- A rendszer az egyes folyamatokhoz/feladatokhoz dokumentum sablonokat generál, a rendelkezésre álló adatokkal feltöltve.
- A munkahelyen kívüli munkavégzés megkapja a szükséges rendszertámogatást, és automatizmust. (https://www.f-consulting.hu, 2020)
- Tekintettel arra, hogy a rendszer könnyen kezelhető, a munkavállalók hamar megtanulják a kezelését, és élvezik előnyeit. (Dr. Kárpáti T., Sárkány Zs.,2009)

A megvalósítás hátrányai:

- A munkavállalók a rendszer betanulási szakaszában sokkal inkább az adminisztrációs terhek növekedését érzik, abból adódóan, hogy új rendszert kell megtanulniuk.
- A nagyobb vezetői kontroll érzete is ellenállást válthat ki. (vidabytes.com/hu, 2022)

Integrált informatikai fejlesztés elmaradásának következményei:

- Nem valósul meg a szervezetben felhalmozódott tudás és információ áramlása sem vertikálisan, sem horizontálisan.
- Nem emelkedik magasabb szintre a különböző szervezeti egységek közös munkavégzése.
- Nem valósul meg a közös munka során a jogosultságok, tárhelyek, valamint a közösen szerkeszthető dokumentumok használata.
- Elmarad a folyamatok, feladatok informatikai rendszerrel való támogatása a magasabb szintű vezetői kontroll.

3.2 Tudásbázis létrehozása projektmenedzsment eszközök használatával

Fontos mindenekelőtt kiemelni, hogy a jó projektmenedzsment nem garancia egy projekt sikerességére, hiszen azt számos belső és külső tényező is befolyásolja, de még az időben, *budget*-ben történő befejezésére sem. A projektmenedzsment célja a folyamatos kontroll fenntartása, a projekt mindenkori státuszának áttekinthetősége, akár visszamenőlegesen is. Valamint a lehetőség megteremtése, hogy utólag levonhassuk a pozitív és negatív tanulságokat. (Prónay G., 2013; Peter L., 2022; Jiwat R., 2022)

3.2.1 Szerepkörök és felelősségek

Egy projektben több szervezet, szervezeti egység és munkatárs dolgozik együtt, akiket a módszertantól függően számos szerepkörhöz lehet, illetve kell is rendelni! Ezen szerepkörök és a hozzájuk tartozó feladatok és felelősségek pontos megértése kulcsfontosságú egy jól működő projektszervezet felállításához.

Projektek végrehajtásának értékelésénél fontos szempont a több oldalról való megközelítés:

- Elméleti, módszertani szempont: a projektvezetés és dokumentáltság szakmaisága.
- Gyakorlati szempont: kellő gondosság és alaposság mellett egy módszertanilag kifogásolható projektmenedzsment is nagyon jó gazdája lehet egy projektnek. Másképp fogalmazva, a módszertani hiányosságok nem feltétlenül okoznak tényleges hátrányokat, azonban a jó projektmódszertan, megfelelő végrehajtással párosulva, kiszámíthatóbbá teszi a projektmenedzsment minőségét. (Jarjabka Á. és társai, 2020; John M. N., 2004; Richard M., 2001)

Személyes tapasztalat, hogy a projektmenedzsment célja és funkciója sajnos sok esetben nem sokkal több, mint a munkával járó feladatok valamely szakterület kollégája általi ütemezése és koordinálása. A projektmenedzsmenttel járó többlet értékek kihasználására csak korlátozottan kerül sor, amennyiben:

- Az eredeti *business case*-ben leírt körülmények és a projekttel szemben támasztott követelmények (felül)vizsgálatára nem kerül sor.
- A kockázatmenedzsment, valamint változás- és problémakezelés csak látszólag van jelen, annak mélysége és minősége nem éri el azt a szintet, hogy tényleges hasznossá váljanak.
- A fejlesztés megvalósítását követően a projektcélok objektív visszamérése és a tanulságok levonása sem történik meg.

A fentiek kodifikálása elengedhetetlen ahhoz, hogy bármilyen vállalat számára az egyetemes tudás részét képezhesse. A legjobb megoldás, ha egy projektirányítási kézikönyv formájában manifesztálódnak az előzőekben leírtak. Enélkül bármilyen projektvezető legfeljebb öncélúan tudna ilyesmikkel foglalkozni, a megfelelő felhatalmazás megléte nélkül.

3.2.2 Kockázat- és problémakezelés

A tudásmenedzsment fentiekben hivatkozott kritériumainak megfelelő integrált informatikai rendszer kifejlesztése és bevezetésé során felmerülő kockázatok rögzítése, hatásvizsgálata - bekövetkezésének valószínűsége, illetve az okozott hatásának mértéke, a kockázatkezelési stratégia, valamint az ehhez kapcsolódó feladatok, felelősök, határidők meghatározása és folyamatos követése, naprakészen tartása az alapvető feladatai a szakszerű kockázatkezelésnek.

Ennek eszköze a kockázatregiszter, mely lehet egy sima táblázat, vagy egy kifejezetten ilyen funkcionalitással rendelkező szoftver (pl. JIRA).

Egy kockázatregiszternek minimálisan az alábbiakat javasolt tartalmaznia:

- a kockázat egyedi azonosítója (sorszáma),
- a kockázat azonosításának (rögzítésének) dátuma,
- a kockázat megnevezése (rövid, leíró elnevezés),
- a kockázat típusa (fenyegetés vagy lehetőség),
- a kockázat hatásának ismertetése (kockázat leírása),
- a kockázat hatásának nagysága (skála szerinti érték),
- a kockázat bekövetkezési valószínűsége (skála szerinti érték),
- a kockázat előbbi két értékből számított mértéke (magas, közepes, stb..)
- a kockázatkezelési stratégia meghatározása, mely a kockázat típusától függően lehet:
    - fenyegetések esetén: elkerülés, csökkentés, áthárítás, megosztás, elfogadás,
    - lehetőségek esetében: kiaknázás, esélynövelés, megosztás, elutasítás,
- a stratégia alapján meghatározott kockázatkezelési intézkedés (azonosítóval),
- az intézkedések adminisztrációja (feladatregiszterben vagy *ticketing* rendszerben),
- feladat megnevezése, leírása, felelőse (feladatgazda), határideje, státusza stb…,
- a kockázatgazda személye,
- a kockázathoz rendelt esetleges határidő és/vagy a legutóbbi státuszváltozás dátuma,
- a kockázat aktuális státusza. (Marcin G., 2020; Akash S., 2022)

Következtetések

A pénzügyi szektor intézményei kiemelkedő jelentőségű, kritikus infrastruktúrák a gazdaság egésze számára. A kezelt vagyon, a saját és ügyfél adatok egyaránt érdekesek és értékesek lehetnek a támadók számára. A támadóknak van idejük a megcélzott rendszer alapos felderítésére, a gyengeségek feltérképezésére.

A pénzintézetek és a náluk tárult információk elleni támadás önmagában is nagy kárt tud okozni, ám elterelő manőverként használva megkönnyíti a további támadó műveleteket. A felhasználók személyes és kártya adatait a pénzintézeteket közvetlenül nem érintő adathalászati technikákkal is meg tudják szerezni. Ezek az ügyfelek bankszámláján vezetett összeg ellopásán túl a pénzintézet elleni támadásra is használhatók.

A támadások mögött nemcsak magánszemélyek, szervezett csoportok, hanem a konkurencia vagy akár idegen kormányok is állhatnak. Ezért az információs vagyon védelméhez komplex rendszerre van szükség.

A pénzügyi szektor szereplői számára egy eredményes és hatékony tudásmenedzsment jelentős szerepet játszik a kiberbiztonság megteremtésében. Elsősorban a szervezeti tudásrendszer létrehozásával, mely a dolgozók, szervezeti folyamatok, szervezeti kultúra, alkalmazott technológia és mindezeket kitöltő, meghatározó tudástartalom összessége. A szervezeti tudásrendszer feladata a tudásfejlesztés, a szervezet tudástárának létrehozása, fejlesztése, és a megfelelő információ hozzáférhetőségének biztosítása megfelelő időben. A szervezet információs, illetve tudásfolyamatainak feltérképezése. A vállalati tudásrendszer megtervezésének feltétele, hogy a szervezet rendelkezzen egy közösen kialakított, előre definiált fogalmi rendszerrel, mely alapján az ismeretek visszakereshetővé válnak.

Hivatkozások

[1] A Microsoft Dynamics 365 Business Central, [Online]. Available: https://navision.hu/. [15 06 2022].

[2] Akash Sureka: Top 14 Features of Atlassian Confluence: A cutting-edge Collaborative Tool, Clarion Blog, [Online]. Available: https://www.clariontech.com/platform-blog/top-14-features-of-atlassian-confluence-a-cutting-edge-collaborative-tool. [16.06.2022].

[3] Anthony J., R.: Knowledge Management in Practice Taylor &Francis Ltd., USA 2022

[4] Az ERP rendszer előnyei és hátrányai a vállalatok számára, [Online]. Available: https://vidabytes.com/hu/ventajas-y-desventajas-de-un-sistema-erp/. [15.06.2022].

[5] BaFin - Bundesamt für Sicherheit in der Informationstechnik, BaFin Perspektiven, Berlin: Bundesamt für Sicherheit in der Informationstechnik, 2020.

[6] Bunkóczi László, Pető István, Pásztor Márta Zsuzsanna, Popovics Attila: Az információs rendszerek szerepe és értékelése a vállalkozásokban, 10.18531/Studia. Mundi, 1. kötet, 1. szám, pp. 3-17, 2015.

[7] Davenport, T.: Enterprise 2.0: The New, New Knowledge Management?". Harvard Business Review. Retrieved 18 April 2013.

[8] Dr. Jarjabka Ákos és társai: Projektmenedzsment ismeretek, Pécsi Tudományegyetem, Közgazdaságtudományi Kar, Vezetés- és Szervezéstudományi Intézet, Pécs, 2020.

[9] Dr. Kárpáti Tibor, Sárkány Zsolt: Az intergrált vállalatirányítási információs rendszerek szerepe a vállalatirányítás hatékonyságának növelésében, Debreceni Egyetem Informatikai Kar, %1. szám [Online]. Available: https://summers.hu/pub/vallir/05.pdf, Debrecen, 2009.

[10] Egyre több a kibertámadás, a bankok viszont nem elég felkészültek, Portfolio.hu, 11.01.2022. [Online]. Available:

https://www.portfolio.hu/bank/20220111/egyre-tobb-a-kibertamadas-a-bankok-viszont-nem-eleg-felkeszultek-520502. [13.05.2022].

[11] Ellie, O: Management of Knowledge-Intensive Organizations, Springer Internacional Publishing AG, USA, 2018.

[12] ERP, avagy a vállalkozások svájci bicskája, 09.12.2020. [Online]. Available: https://www.f-consulting.hu/erp-avagy-a-vallalkozasok-svajci-bicskaja/. [15.06.2022].

[13] Evans, Lester, Cybersecurity: An Essential Guide to Computer and Cyber Security for Beginners, Including Ethical Hacking, Risk Assessment, Social En, New York: Bravex Publications, 2020.

[14] Fred Imbert, Jeff Cox, Pippa Stevens: CNBC, 11. 02.2020. [Online]. Available: https://www.cnbc.com/2020/02/11/stock-market-today-live.html. [09.05.2022].

[15] Girard, John P.; Girard, JoAnn L.: Defining knowledge management: Toward an applied compendium (PDF), Online Journal of Applied Knowledge Management. 3 (1): 14., 2015.

[16] Holsapple, Clyde (Ed.): Handbook on Knowledge Management, Knowledge Matters, Springer-Verlag Ltd, Berlin, 2003, (ISBN 978-3-540-24746-3)

[17] Jiwat Ram: Project manager – project staff fit: Does it matter?, 15.03.2022. [Online]. Available: https://www.ipma.world/project-manager-project-staff-fit-does-it-matter/. [16 06 2022].

[18] John M. Nicholas: Project Management for Business and Engineering, Loyola University Chicago, ISBN: 0-7506-7824-0, Elsevier Inc., Amerikai Egyesült Államok, 2004.

[19] Leah Costello: Benefits of ERP: Advantages, Disadvantages & Selecting an Enterprise Resource Planning System, 16.03.2022. [Online]. Available: https://terillium.com/benefits-of-erp/. [16 06 2022].

[20] Marcin Geb: Risk management in Jira. How to locate a decent plugin?, 05.06.2020. [Online]. Available: https://bigpicture.one/jira-risk-management/. [16.06.2022].

[21] Mihály, Zala: Sosem látott támadások várnak a pénzintézetekre, ey.com, 12 04 2021. [Online]. Available: https://www.ey.com/hu_hu/cybersecurity/sosem-latott-tamadasok-varnak-a-penzintezetekre. [13 05 2022].

[22] Nonaka, Ikujiro, von Krogh, Georg: Tacit Knowledge and Knowledge Conversion: Controversy and Advancement in Organizational Knowledge Creation Theory, Organization Science. 20 (3): 635–652, 2009.

[23] Peter Landau: Top 20 Project Management Skills for 2022, [Online]. Available: https://www.projectmanager.com/blog/project-management-skills. [16 06 2022].

[24] Prónay Gábor: Tudásmenedzsment szerepe a projektekben, [Online] Available: http://blog.mfor.hu/projekt/6406.html, 2013.

[25] Richard Murch: Project Management, Best practices for IT professionals, Prentice Hall PTR, Upper Saddle River, ISBN: 0-13-021914-2, Amerikai Egyesült Államok, 2001.

[26] Richard Samans, Jane Nelson: Integrated Corporate Governance: Six Leadership Priorities For Boards Beyond The Crisis, World Economic Forum, 18.06.2020. [Online]. Available: https://www.forbes.com/sites/worldeconomicforum/2020/06/18/integrated-corporate-governance-six-leadership-priorities-for-boards-beyond-the-crisis/. [15.06.2022].

[27] Rohmeyer, Paul; Bayuk, Jennifer L., Financial Cybersecurity Risk Management Leadership Perspectives and Leadership Perspectives and Institutions, New York: Springer-Apress, 2019.

[28] Skala, K., Davidović, D., Afgan, E., Sović, I. &; Šojat, Z.: Scalable Distributed Computing Hierarchy: Cloud, Fog and Dew Computing. In: Open Journal of Cloud Computing (RobPub) 2 (1): 16–24., 2015., ISSN 2199-1987

[29] Skoll: A tudásmenedzsment fogalma és lényege, 22.10.2021. [Online]. Available: https://skoll.hu/tudasmenedzsment/. [17.05.2022].

[30] Vállalatirányítási rendszer, [Online]. Available: https://www.acterra.hu/vallalatiranyitasi-rendszer/. [15.06.2022].

[31] vallalatiranyitasi-rendszer.hu: Az integrált vállalatirányítási rendszer fogalma, [Online]. Available: https://vallalatiranyitasi-rendszer.hu/integralt-vallalatiranyitasi-rendszer/. [15.06.2022].

[32] Wapenaar J.: TOPdesk, 17.05.2022. [Online]. Available: https://www.topdesk.com/hu/fogalomtar/mi-a-tudasmenedzsment/

[33] Yates P: Knowledge Management: Theory and Practice, Clanrye International Ltd, USA, 2022