International Journal of Engineering and Management Sciences (IJEMS) Vol. 1. (2016). No. 1.
DOI: 10.21791/IJEMS.2016.1.17.

Információbiztonság szerepe az üzleti folyamatokban
The role of information security in the business processes

S. DOMBORA[1], P. MICHELBERGER[2]

[1]Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, Híradástechnikai Intézet, dombora.sandor@kvk.uni-obuda.hu
[2]Óbudai Egyetem, Keleti Károly Gazdasági Kar, Szervezési és Vezetési Intézet, michelberger.pal@kgk.uni-obuda.hu

Absztrakt. Az információbiztonság (üzleti adatok bizalmassága, sértetlensége és rendelkezésre állása) napjainkban egyre fontosabb a vállalatok számára. Elérése azonban nem öncélú. A vállalatok biztonságos működésüket szeretnék ezzel (is) magalapozni. A tanulmány két rövid információbiztonsági tevékenységet tárgyaló esettanulmány bemutatása mellett áttekinti a folyamatbiztonsághoz köthető fogalmakat és menedzsment tevékenységeket. Az információvédelmi szabályozások kapcsán megismert üzletmenet-folytonossági tervek és kockázatkezelési eljárások a vállalat összes üzleti folyamatára kiterjeszthetők.

Abstract. Information security (namely, confidentiality, integrity, and availability of business-related data) is an issue which companies attach increasing importance nowadays. This is, however, not a self-centred goal to achieve, but an (additional) means businesses use to work towards security in their overall operations. In addition to briefly presenting two case studies on information security practices, this paper offers a survey of terms and management practices linked with process security. Business continuity planning and risk management techniques - as outlined here in connection with information protection controls - may cover all business processes at any company.

Bevezetés

A vállalatok megbízható működésre, az üzleti partnerek igényeinek időben, mennyiségben és minőségben történő kielégítésére törekednek. Feltérképezik vállalati folyamataikat, értékteremtéshez szükséges eszközeiket és ezek rendelkezésre állását. Csak az erőforrások (köztük a kiemelt szerepet kapó információ) biztosításával lehet az értékteremtő üzleti folyamatokat végrehajtani. A vállalat és folyamatainak biztonságmenedzsmentje olyan folyamatos tervezési, szervezési, irányítási és ellenőrzési tevékenységet jelent, amely a vállalat minden külső és belső érintettje számára elfogadható és fenntartható biztonsági szintet jelent.

A vállalati versenyképesség alapvető, de nem kizárólagos tényezője a nyereséges gazdálkodás. A tartós működőképesség feltételezi, hogy a vállalat törekszik a biztonságra. Ebben fontos szerepet kapnak a vállalati folyamatok és azok ügyviteli leképezése, úgynevezett workflow-ja. A szervezetek legfőbb

DOI: 10.21791/IJEMS.2016.1.17.

biztonsági kockázata az ember. A folyamatbiztonság csak úgy érhető el, ha folyamatokban résztvevők munkáját szabályozzuk, ill. felkészítjük őket nem várt kockázati események kezelésére.

1. Folyamatközpontúság

„A folyamat egy vagy több tevékenység, amely értéket növel úgy, hogy egy bemenetkészletet átalakít a kimenetek készletévé (javakká vagy szolgáltatásokká) egy más személy (a vevő, ill. felhasználó) számára, emberek, módszerek és eszközök kombinációjával." [13, p. 75.]

Folyamatbiztonság olyan állapotnak tekinthető, ahol az előírt bemenetek (folyamat végrehajtásához szükséges erőforrások) biztosítása után a folyamat tevékenységeit végrehajtó szervezeti egységek az előírt időben megfelelő mennyiségű és minőségű kimenetet (termék, szolgáltatás, információ) nyújtanak és zavar esetén a folyamat normál működése a lehető legkisebb erőforrás ráfordítással és a legrövidebb idő alatt helyreállítható.

2. Üzletmenet folytonosság

Az üzletmenet folytonosság esetében a szervezet folyamatai zavartalanul és hibamentesen működnek és az azokhoz szükséges erőforrások megfelelő helyen és időben rendelkezésre állnak. A szervezetek elsősorban információbiztonsági vonatkozásban használják a fogalmat és az ún. „üzletmenet-folytonossági terv" információvédelmi intézkedéseket tartalmaz (bizalmasság, sértetlenség és rendelkezésre állás). Célja a szervezeti folyamatokat támogató (informatikai) erőforrások meghatározott időben és funkcionális szinten történő rendelkezésre állásának biztosítása, valamint váratlan eseményekből bekövetkező károk minimalizálása. Számba veszi a folyamatok fenyegetettségeit, ezek bekövetkezési valószínűségét és a folyamat kieséséből eredő károkat. Megadja a lehetséges helyettesítő eljárásokat, amíg a helyreállított folyamat újra nem indul.

Minden folyamat végrehajtásához erőforrásokra van szükség, amelyek közül kiemelkedik a megfelelő helyen és időben, a jogosult személyek számára biztosított információ. A vállalati folyamatokat virtuálisan leképező információs rendszerek szabályozott működtetésével elérhetjük a folyamatok biztonságát. A szűken értelmezett információtechnológiai megközelítés azonban kiterjeszthető bármelyik más vállalati folyamat feltételeinek biztosítására, annak előírásszerű végrehajtására vagy zavar esetén normál működésének helyreállítására. A folyamatszemléletű üzletmenet-folytonosság nem csak információbiztonsági problémákra alkalmazható [1].

Napjainkban a vállalatok üzletmenet-folytonosságát növekvő számú és egyre nehezebben átlátható veszély fenyegeti. Minden üzleti folyamatot (pénzügyi, működési, stratégiai és projekt-) és kapcsolódó erőforrást (ember, IT, berendezések, infrastruktúra, energia, üzleti partnerek) kockázatelemzésnek és -kezelésnek kell(ene) alávetni [15]

A klasszikus Porter féle értéklánc modell [7] alapján a folyamatok végrehajtását biztosító szervezeti erőforrásokat három lépésben vizsgálja;

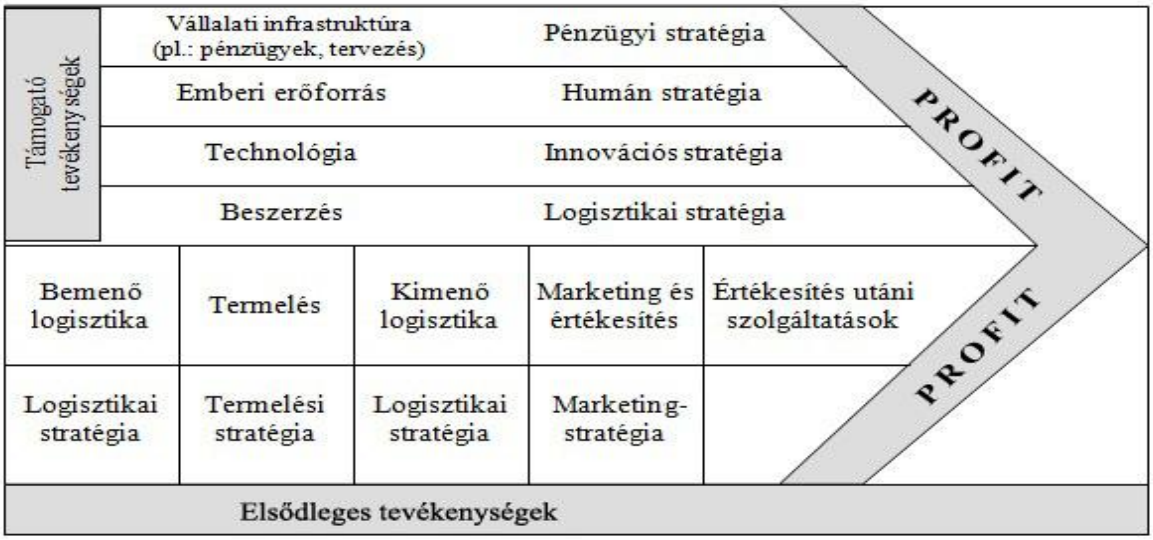
1. meghatározza, hogy a kimenetek létrehozásában milyen tevékenységek (folyamat elemek) játszanak szerepet,

DOI: 10.21791/IJEMS.2016.1.17.

2. elemzi, hogy ezek a tevékenységek hogyan járulnak hozzá a kibocsátás értéknöveléséhez,
3. vizsgálja, hogy a szervezetek mennyit kötnek le erőforrásaikból és ezek milyen költséget jelentenek.

Itt a nyereségesség mellett előkerül(het)nek biztonságos működést, ill. üzletmenet folytonosságot érintő kérdések is.

A folyamatokat ez a modell alapvetően két csoportba sorolja. Szétválasztásuk nem könnyű, de az elsődleges tevékenységek a fogyasztó vagy vevő érdekeiben történik, míg a támogató tevékenységek a szervezet működését szolgálják. Az üzleti tankönyvek az elsődleges tevékenységekhez a beszerzést, belső logisztikát, a technológiai átalakítást, a külső logisztikát, a marketing és értékesítési tevékenységet valamint a vevőknek nyújtott kapcsolódó szolgáltatásokat sorolják. A támogató tevékenységek az elsődleges tevékenységek végrehajtásához járulnak hozzá (pl. szervezetfejlesztés, vezetési feladatok és stratégiai tervezés). A folyamatok csoportosítása segítheti a kockázati tényezők feltárását, de kockázati tényezők (fenyegetések) értékelésénél holisztikus szemléletben kell elvégezni figyelembe véve a folyamatok kölcsönhatásait is.



1. ábra: Porter féle értéklánc modell

(Forrás: [7])

4. Versenyképesség és minőség

„Egy nemzetgazdaságban azokat a vállalatokat tekintjük versenyképesnek, amelyek társadalmilag elfogadható normák betartása mellett a számukra elérhető erőforrásokat minél nagyobb nyereségfolyammá képesek transzformálni, képesek a működésüket befolyásoló környezeti és vállalatukon belüli változások észlelésére és az ezekhez való alkalmazkodásra annak érdekében, hogy a nyereségfolyam lehetővé tegye tartós működőképességüket.” [3, p.31.]

A meghatározás a vállalati versenyképesség alapvető, de nem kizárólagos tényezőjének a nyereséges gazdálkodást tekinti. A tartós működőképesség feltételezi, hogy a vállalat törekszik a biztonságra, a

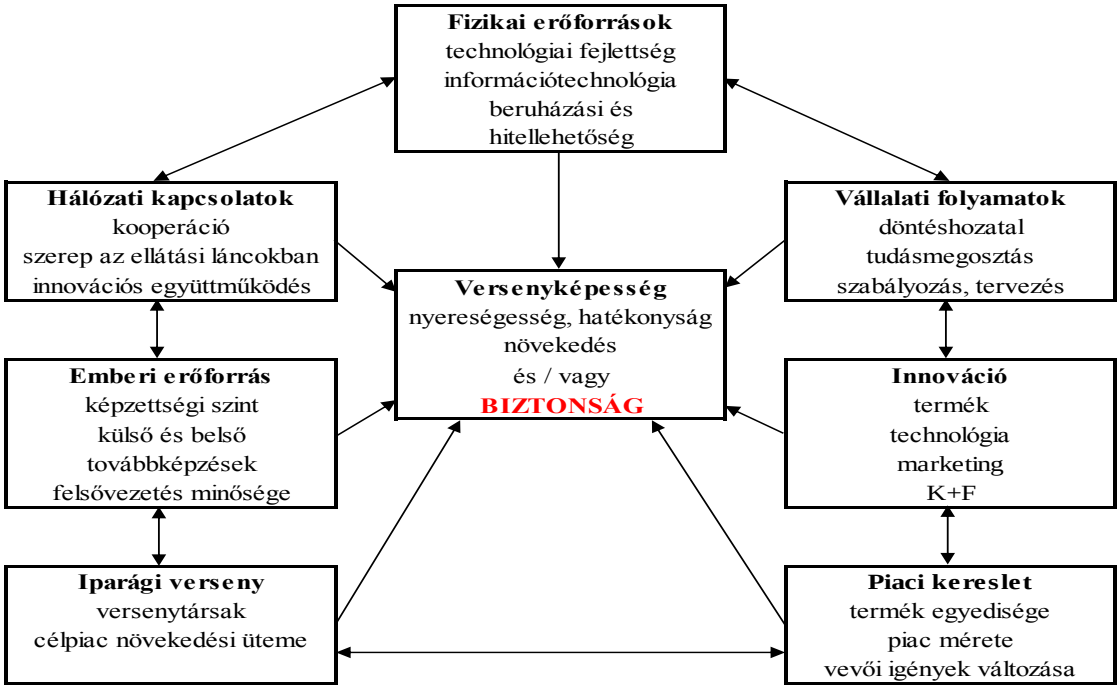
DOI: 10.21791/IJEMS.2016.1.17.

fizikai és emberi erőforrások, a vállalati folyamatok, az innováció, a piaci kereslet és a vállalat közvetlen környezete szempontjaiból egyaránt.

A vállalatok versenyképességét nagymértékben befolyásolja a folyamatok végrehajtásának időigénye és az előállított kimenetek (termékek, szolgáltatás, információ) minősége. Egyre fontosabb szerepet játszik a minőség és annak biztosításához szükséges minőségmenedzsment. A minőségi kimenet előállítása optimális ráfordítás mellett függ a vállalat munkafolyamatainak dokumentáltságától, szabályozottságától és automatizáltságától. Fontos szerepet játszik az egyes kimenetek előállítása során elvégzett feladatok dokumentálása [9]. Ez lehetővé teszi az előállított kimenetek életútjának nyomon követését, a hibásan elvégzett feladatok azonosítását, az összegyűjtött adatokból számított statisztikák alapján pedig a leggyakoribb hibák azonosítását valamint a munkafolyamatok megújítását, optimalizálását.

A vállalati folyamatok végrehajtása közben a folyamatlépések elvégzése során a munkatársaknak és partnereknek pontos adatokra van szükségük a feladataik végrehajtásához. Ezek az adatok üzleti titkot képező információt hordozhatnak. Kezelésük, tárolásuk és továbbításuk kiemelt figyelmet igényelhet. Az adatok bizalmasságának megőrzése [13] befolyásolhatja a vállalat versenyképességét, kiszivárgása veszélyeztetheti a vállalat működését és fennmaradását.

A folyamatok végrehajtásához szükséges adatok hiánya [5], hiányossága és pontatlansága az előállított kimenetek minőségének romlásához vezethet, amely megrengetheti a vevők bizalmát a vállalat termékeiben illetve szolgáltatásaiban. A vállalat keretében működő minőségirányítási rendszernek biztosítania kell, az adatok rendelkezésre állását, sértetlenségét és nem utolsó sorban a bizalmasságát is, egyszóval támogatnia kell a folyamatok végrehajtásához szükséges információ biztonságát.



2. ábra: Versenyképességi modell

(Forrás: [11])

DOI: 10.21791/IJEMS.2016.1.17.

5. Versenyképesség és folyamatautomatizálás

Felgyorsult világunkban nagy szerepet játszik a munkafolyamatok kimeneteinek előállítására fordított munkaidő és költség. A versenyképesség megőrzésének érdekében jó stratégiának tűnik a folyamatok által előállított kimenetekre fordított munkaidő és költség csökkentése a minőség javítása mellett. Az emberi erőforrás a legdrágább, így jó alternatíva a vállalati folyamatok automatizálása.

A folyamatok automatizálásával lehetővé válik a munkafolyamatok feladatainak pontos ismétlése, nő a termelékenység, javul és stabilizálódik minőség valamint nő a folyamatbiztonság. Ugyanakkor a termelési, üzleti és ügyviteli folyamatok automatizálásához automatizálási infrastruktúrára van szükség. Ezt az infrastruktúrát informatikai rendszerek vezérlik, amelyek megfelelő beállítása és programozása kiemelt figyelmet és ellenőrzést igényel az üzemeltetők részéről. Fontos szerepet játszik a feladatok végrehajtásához szükséges információ, megfelelő helyre megfelelő időben való eljuttatása. A hiányos, sérült vagy hibás adatok felhasználása hibás termékek és szolgáltatások előállításához, adott esetben akár a folyamat leállásához is vezethet, amely jelentős kárt okozhat a vállalatnak.

A beállításokon és programozáson túl, fontos szerepet játszik az automatizálást lehetővé tevő infrastruktúra és a vezérlő rendszerek minősége [2]. A megoldás-szállítók törekednek a megfelelő minőségű hardver és szoftver elemekből álló automatizálási infrastruktúra előállítására, de a folyamatos versenyhelyzet, a termékek mielőbbi piacra juttatására sarkallja őket. Ez adott esetekben a regressziós tesztelések elmaradásához, ez által a kész automatizálási termékek részleges teszteléséhez vezethet. A technológia gyors fejlődése, a hiányos, vagy tévesen összeállított tesztforgatókönyvek segítségével ellenőrzött automatizálási infrastruktúrák, a tesztelések teljes körűségének hiánya, új veszélyforrások megjelenéséhez vezet. Előfordulhatnak olyan infrastruktúra vagy vezérlési hiányosságok és hibák, amelyek hibás output előállításához, adott esetben személyi sérüléshez vezethetnek. Ezek kivédésére a megoldás-szállítók folyamatosan fejlesztik és tesztelik az előállított infrastruktúrát, szükség esetén szoftveres javítócsomagokat állítanak össze és küldenek vásárlóiknak a már megvásárolt és üzembe helyezett infrastruktúra karbantartásához.

A számítógép vezérelte, programozható automatizált infrastruktúrák lehetőséget nyújtanak különböző kimenetek váltakozó előállítására. A különböző kimenetek különböző munkafolyamatok végrehajtását igénylik. A különböző munkafolyamatok implementálása az automatizálási infrastruktúrában feltételezi a munkafolyamatok részletes ismeretét, amelyet:

- működő folyamatok esetében a munkavégzés során elvégzett feladatok elemzésével és leírásával,
- új folyamatok esetében, a folyamat részletekbe menő megtervezésével és dokumentálásával lehet elérni.

A folyamatok végrehajtása előtt fontos szerepet játszik a munkafolyamat teszt jellegű végrehajtása és az előállított kimenetek ellenőrzése. A megfelelően tesztelt, automatizált infrastruktúra és infrastruktúra implementálás hozzájárul a magas minőségű kimenetek optimális időben való előállításához.

DOI: 10.21791/IJEMS.2016.1.17.

6. Folyamat-végrehajtás és információbiztonság

A feladatok végrehajtásához elengedhetetlen a tevékenységek elvégzéséhez szükséges útmutatók és erőforrások rendelkezésre állása. Fontossá válik a folyamatlépések dokumentációjának eljuttatása a feladatot végrehajtó illetékes munkatársakhoz, amely megfelelő részletességgel tartalmazza szükséges erőforrások listáját és a tevékenységek végrehajtásának módját [6].

A folyamatok zökkenőmentes végrehajtásához időben biztosítani kell, a megfelelő mennyiségű és minőségű erőforrást a kijelölt munkahelyekre [14]. Az erőforrások logisztikája kulcsszerepet játszik a folyamatos működés megvalósításában, amelyhez megbízható információra és logisztikai rendszerre van szükség. Az erőforrások egy része sok esetben információ, amely csak a feldolgozó személyek számára megismerhető.

A folyamatok végrehajtásának és az információ feldolgozásának érdekében a vállalatok folyamatokat támogató eljárásrendeket és szabályzatokat alkotnak. A szabályzatoknak a feldolgozandó információ bizalmassági besorolásának megfelelő módon kell kezelniük az információ védelmét. Ha a folyamat végrehajtása során adatfeldolgozás történik, a folyamat végrehajtását szabályozó eljárásrendeknek részletesen ki kell térniük az információbiztonság megvalósítására. Kritikus adatok feldolgozása esetén minden folyamatlépés leírásnak tartalmaznia kell az információt feldolgozó személyek adatokkal kapcsolatos jogosultságait [10]. Ez esetben szerepkör alapú jogosultsági rendszer kialakítására van szükség, amelyben az egyes adatokhoz való hozzáférés lehet teljes körű vagy részleges. Az írási és olvasási jogosultságoknak el kell különülniük egymástól (bizonyos attribútumok csak olvashatók és bizonyos attribútumok írhatók). Például, ha személyes adatok tárolása és feldolgozása történik a folyamat végrehajtása során, az adatok védelmét jogszabályok határozzák meg, ez esetben a szabályzatoknak részletesen tárgyalniuk kell a jogszabály által előírt adatvédelmi céloknak megfelelő feldolgozási rendet.

Az alkalmazott folyamat automatizálást támogató infrastruktúráknak biztosítaniuk kell az információbiztonsági követelményeknek megfelelő jogosultsági rendszer kiépítését. A felhasználóknak a szükségesnél csak bővebb jogosultságot lehetőtővé tevő folyamat automatizálási infrastruktúrák nagyobb teret engednek a platform független úgynevezett social-engineering támadásoknak.

A folyamatok végrehajtása során a kimenetek előállításával egy időben a minőségirányítási rendszer további, a kimenet előállításhoz kapcsolódó adatokat gyűjt, amelyek feldolgozásával javítható a kimenetek minősége és optimalizálható a folyamatok végrehajtása. Fontos szempont, hogy a folyamatok dokumentációi, a folyamat végrehajtás során keletkezett minőségügyi információk bizalmasak, belső használatúak. Ha konkurenciához kerülnek, az versenyelőnyre tehet szert annak felhasználásával.

A folyamat szemléletű információbiztonság kialakítása azt célozza meg, hogy megvalósuljon az információ védelme a folyamatok végrehajtása során. Ennek érdekében a részletes folyamat felmérés, tervezés és dokumentálás során összegyűjti az feldolgozott adatokra vonatkozó biztonsági követelményeket. A folyamatlépések végrehajtását és a végrehajtói szerepköröket úgy alakítja ki, hogy az megfelelő szintű információbiztonságot eredményezzen. A folyamat végrehajtást támogató

DOI: 10.21791/IJEMS.2016.1.17.

rendszerek implementálása során követelményeket támaszt az információbiztonsági architektúra tervezésével kapcsolatban és a rendszer elkészítését követően teszteli annak biztonsági követelményeit. Kész automatizálási rendszer vásárlása esetén az információbiztonság megvalósítását a beszerzendő rendszerrel szemben megfogalmazott biztonsági követelmények formájában támogatja.

A legújabb Európai Uniós trendek nagy hangsúlyt fektetnek az információbiztonságra. Korábbi kutatásaink és fejlesztési projekt auditjaink azt igazolták vissza, hogy az informatikai rendszerekben megjelenő információbiztonsági hiányosságok a biztonsági tervezés hiányára vagy hiányosságaira vezethetők vissza. Az ENISA (European Union Agency for Network and Information Security) gondozásában megjelent „Privacy and Data Protection by Design" tervezési modelleket mutat be [4], amelyek elősegítik az adatok és személyes információk védelmét az informatikai rendszerekben. A tanulmány kitér az adatvédelmi tervezési stratégiára, és technológiai szinteken rendelkezésre álló biztonsági technológiákra és technikákra.

7. Kockázatértékelés és -kezelés

A kockázatelemzés és csökkentés alapja szakirodalomban ALARP (As Low As Reasonably Practicable) néven ismert és inkább műszaki területen alkalmazott alapelv lehet [8]. A műszaki rendszer tervezőjének törekednie kell a lehető legkisebb, még ésszerűen megvalósítható kockázati szint elérésére.

3. ábra: ALARP alapelv

(Forrás: [8: 6])

DOI: 10.21791/IJEMS.2016.1.17.

Ha a kockázat túl magas, nem csökkenthető és elfogadhatatlannak látszik, akkor egyedüli lehetőség az elkerülés.

Ha csökkenthető a káros esemény bekövetkezésének valószínűsége vagy a káresemény pénzben kifejezett nagysága, akkor a szervezet megpróbálja a kockázatot az elfogadható szintre szorítani. Ebben az esetben elsősorban a kockázatot kiváltó okokat próbálják kezelni. A kockázatcsökkentés azonban nem mindig lehetséges, vagy annak költsége aránytalanul magas, esetleg nem hoz számottevő eredményt. Ezekben az esetekben jelenthet megoldást a kockázat más szervezetekkel történő megosztása) (pl. beruházásnál fővállalkozó megbízása) vagy esetleges áthárítása (pl. biztosítás). Ez utóbbiak a kockázat finanszírozását igénylik.

A menedzsment sok esetben tudatosan vállalja, viseli a szervezet kockázatait, ami egy elfogadott és folyamatosan ellenőrzött kockázati szintet jelent.

8. Esettanulmányok

8.1 Sikeres IT eszközgazdálkodás bevezetése

A projekt célja: Egy több ezer ügyfelet kiszolgáló ITIL alapú IT szolgáltatásmenedzsment megoldás keretében megvalósított konfigurációkezelésre épülő integrált IT eszközgazdálkodási megoldás kialakítsa, egy informatikai szolgáltatónál.

Követelmények:

- konfigurációs adatbázis kialakítása a meglévő IT szolgáltatásmenedzsment rendszerben;
- munkafolyamatok eszközadatok naprakészen tartásához;
- szigorú számozású eszközmozgás bizonylatok (bevételezés, kiadás, mozgatás, selejtezés) előállítása és nyomtatása egyedi és tömeges módon;
- eszközök adatainak automatikus frissítése a konfigurációs adatbázisban – integrált igény és változáskezelés keretében;
- a kiszolgálás során az eszközt kezelő személynél legyen a felelősség papíron is;
- a folyamatokban részt vevő személyek csak a saját ügyfélkörükhöz kapcsolódó eszközökhöz férjenek hozzá (lássák, mozgathassák);
- az eszközgazdálkodók mindent láthassanak és módosíthassanak (eredeti igény szerint még a raktárkészletet is);
- leltározás támogatási funkció;
- eszköz összeépítés funkció;
- eszközök foglalása a mozgatás idejére (ne lehessen más eszközmozgást kezdeményezni rájuk);
- lehetőség a hiányzó adatok pótlására és hibás adatok javítására az eszközmozgatások során;
- eszközök könyvelése ügyfélre, munkatársakra és projektre;
- főkönyvi feladások elkészítése az eszközmozgás bizonylatok alapján.

DOI: 10.21791/IJEMS.2016.1.17.

Adottság, hogy az informatikai szolgáltató több tízezer ügyfél felhasználót szolgál ki, több mint 100 szervezetnél.

A projekt indulásakor rendelkezésre álló műszaki feltételek:

- meglévő ITSM (IT Service Management) megoldás, amelynek keretében működött az incidenskezelés és igénykezelés;
- a meglévő ITSM megoldás rendelkezett konfigurációkezelési modullal és testre-szabható konfigurációkezelési adatbázissal;
- üres konfigurációs adatbázis az ITSM rendszerben;
- hiányos eszközadatok részleges rendelkezésre állása a meglévő ERP rendszerben;
- folyamatban lévő leltár több mint 30.000 eszköz esetében;
- túlbonyolított eszközgazdálkodási folyamatok, amelyek nem alkalmasak nagy mennyiségű eszköz kezelésére, továbbá visszaélésekre adott lehetőséget az eszközgazdálkodók számára;
- eszközgazdálkodók és kiszolgáló személyzet biztonságtudatosságának hiánya;
- több mint 10 eszközgazdálkodó;
- több mint 200 kiszolgáló személy;
- több eszközraktár, sok ügyfél helyszín;
- több mint 10 féle eszközmozgás típus főkönyvi megfelelővel.

Végrehajtott feladatok a projekt során:

- eszközgazdálkodási és konfigurációmenedzsment folyamatok felmérése, optimalizálása, összehangolása és dokumentálása beleértve a szerepkörök kialakítását;
- a szerepkörök kialakítása során kiderült, hogy az eszközök és felhasználók adatai bizalmas adatot képeznek, így szerepkör függő eszköz attribútum hozzáférés kialakítást kellett megvalósítani;
- kiderült, hogy az eszközgazdálkodói szerepkör jogosultsága lehetővé teszi a raktárkészletek módosítását, így szükség volt egy olyan folyamat kidolgozására, amely biztosította, hogy a módosítás csak a raktárosok értesítésével/jóváhagyásával történhessen;
- minden folyamatlépésben meg kellett határozni a folyamat szereplőit, a feladatokat végrehajtók jogosultságait (milyen eszközöket mozgathat, azoknak milyen adatait láthatja, kik lehetnek az eszközök átadói és átvevői);
- munkafolyamatok és konfigurációs adatbázis implementálása;
- elkészült rendszer bevezetése és feltöltése adatokkal.

A folyamatok definiálása során, a jogosultsági rendszer kialakítása, az információ biztonságának (bizalmasság, sértetlenség és rendelkezésre állás) biztosítása jelentette a legnagyobb kihívást. A problémák részletezve:

- a folyamatok pontos specifikálása és a jogosultsági rendszer kialakítása során az ügyfél nem ismerte fel a biztonsági követelmények szükségességét;
- az ügyfél sokkal több jogosultságot kért az eszközgazdálkodási és konfigurációkezelési szereplők számára egyes folyamatlépések során, ami visszaélésre adhatott volna lehetőséget;

DOI: 10.21791/IJEMS.2016.1.17.

- adatok integritásának biztosítása a folyamatlépések végrehajtásának során, azaz csak engedélyezett módosítások történhessenek az adatokon.

Eredmények:

- jól működő eszközgazdálkodási folyamatok, amelyek végrehajtása lehetővé tette a munkafolyamatok hatékony végrehajtását a dokumentálás minimalizálása mellett;
- információbiztonságot szolgáló jogosultsági rendszer, amely biztosítja a bizalmas eszköz és személy adatok védelmét, valamint az adatok integritását;
- a pontos felmérésnek és részletes dokumentálásnak köszönhetően a fejlesztés gyorsan haladt, az elkészült funkciók megfeleltek az elvárásoknak;
- a kialakított rendszer első éves üzemelése során nagymértékben javult az eszközadatok minősége.

Összegzés

A kihívások ellenére, a minőségi követelményspecifikáció és a részletes tervezés sikeres projektzárást eredményezett. A rendszer kielégítette a működési folyamatok dokumentációs igényeit, amelynek működőképességét a dokumentáció előállításához szükséges feladatok minimalizálásával, az adatok összegyűjtésének automatizálásával sikerült elérni.

8.2 Sikertelen vállalatirányítási rendszer bevezetés

A projekt célja: Integrált vállalatirányítási rendszer kialakítása egy sportszervezetnél, amely biztosítja a korábban működő vállalatirányítási rendszer funkcióit és biztosítja a rendszerben tárolt személyes adatok védelmét.

Követelmények:

- jelen rendszer funkcióinak kiváltása, biztonságos, adatvédelmi követelményeket teljesítő informatikai megoldással;
- modern, biztonságos szoftver- és hardver-infrastruktúra kialakítása;
- információbiztonság és magas rendelkezésre állás növelése;
- partner szervezetekkel való biztonságos elektronikus kapcsolat kialakítása, elektronikus ügyintézés támogatása;
- működési folyamatok felhasználói szintű támogatása.

Adottság, hogy a szervezet a rendszerben több ezer személyes adat kezelését végzi, meg kell felelnie az adatvédelmi jogszabályoknak.

A projekt indulásakor rendelkezésre álló feltételek:

- egyéni igények (kevés a piacon rendelkezésre álló kész megoldás);
- a fejlesztés a meglévő rendszer alapján ígéretesnek mutatkozott;
- heterogén, nagy létszámú, kevés információbiztonsági és adatvédelemi tudással rendelkező felhasználó;

DOI: 10.21791/IJEMS.2016.1.17.

- komplex dokumentált működési folyamatrendszer - amely csak szervezeti egység szinten tér ki a folyamatbeli feladatok végrehajtóira - nincsenek dedikált feladat végrehajtói szerepkörök definiálva, a felelősségek és végrehajtók nincsenek meghatározva;
- a régi rendszer cseréje az integrált rendszerműködés, elektronikus ügyintézés megvalósítása és információbiztonsági okokból történik.

Végrehajtott és elmulasztott feladatok:

- részleges követelményspecifikáció elkészítése a meglévő rendszer és dokumentáció alapján;
- információbiztonsági és adatvédelmi igények felmérésének elmulasztása;
- jogszabályi követelmények felmérésének elmulasztása;
- rendszertervezés a hiányos követelményspecifikáció alapján;
- fejlesztés a meglévő rendszer hiányos dokumentációja és az információbiztonsági igények hiányos felmérése és tervezése mentén;
- tesztesetek és tesztelési eljárások hiányos összeállítása – csak a végrehajtható forgatókönyvek kerültek be a tesztforgatókönyvekbe, kimaradtak a negatív tesztesetek és a biztonsági tesztek.

Kihívások:

- információbiztonsági architektúra és adatvédelmi funkciók kialakítása;
- jogosultsági igények felmérésének elvégzése: folyamat – feladat – szerepkör – jogosultság összerendelési információk felmérése és meghatározása;
- komplex igényeknek megfelelő jogosultsági rendszer megtervezése;
- feladatonkénti szerepkörök jogosultsági körének meghatározása;
- adatvédelmi jogszabályi követelmények dokumentálása, szükségességének felismerése;
- adatok bizalmassági besorolásának felismerése (attribútum szintű jogosultsági követelmények);
- a problémák folyamatos felbukkanásának hatására, amelyeket a szállító nem tudott értelmezni, kommunikációs problémák léptek fel a megrendelő és szállító között;
- nem megfelelő projekt menedzsment, ami miatt folyamatos csúszás következett be, a megrendelő bizalmának elvesztéséhez vezetett.

Eredmény, hogy az elkészült rendszer többszöri határidő módosítás után került átadásra (mennyiségi átadás) tesztelésre.

A tesztelés során az alábbiakat tapasztalta a megrendelő:

- a hiányos követelményspecifikáció miatt eltérően értelmezte a funkciókat a szállító és a megrendelő;
- a felhasználói csoportok képernyőkhöz és nyomógombokhoz rendelése a feladat és funkció alapú jogosultsági rendszer helyett;
- adatvédelmi jogszabályban megfogalmazott követelmények figyelmen kívül hagyása;
- hiányos rendszertervezés, felületes működési folyamat leírások;
- kritikus biztonsági hiányosságok;
- tesztelési hiányosságok miatt nagyobb terhelés a megrendelői tesztelés során;

DOI: 10.21791/IJEMS.2016.1.17.

- több száz funkcionális hiba az átadott rendszerben;
- információbiztonsági követelmények megsértését lehetővé tevő architektúra;
- hiányos dokumentáció: rendszerterv, fejlesztői specifikáció, minőségbiztosítási terv, projektterv;
- OWASP (Open Web Application Security Project) módszertan szerinti sérülékenység vizsgálat szinte minden elvégzett tesztje sérülékenységet jelzett.

Összegzés

A fejlesztés és az információbiztonság megvalósításának minőségét nagymértékben befolyásolja a projekt során elkészített dokumentációk minősége és teljessége. Kijelenthetjük, hogy a részletesen megfogalmazott, pontosan definiált követelmények alapját képezik a rendszer, folyamat és információbiztonságnak. Az elkészült termék biztonsági hiányosságai nem tették lehetővé annak bevezetését, további fejlesztések váltak szükségessé a termék biztonságossá tételének érdekében.

Összefoglalás

A vállalti folyamatok típusától függetlenül, mindegy, hogy azok ügyfél kiszolgálást vagy működéstámogatást valósítanak meg, kiemelt szerepet játszik az információbiztonság. A termelési folyamatok esetében az információ rendelkezésre állásának hiánya gyártósori leállást így termeléskiesést okozhat, amely jelentős anyagi kárral társulhat. Az információ bizalmasságának megőrzése főleg a személyes adatokat kezelő szervezetek esetében kritikus, amelyet jogszabály ír elő, de a belső információk konkurenciához való eljutása versenyhátrányhoz vezethet. A hibás vagy sérült adatok hibás termékek előállítását, személyi sérülést okozhatnak. Összességében elmondható, hogy az információbiztonság alapvető követelményként jelenik meg a vállalati folyamatok végrehajtásának biztonságát illetően és ez által befolyásolja a vállalat versenyképességét is.

Hivatkozások

[1] J. Ø. Aagedal, F. den Braber, T. Dimitrakos, A. Gran, Bjørn, D. Raptis, K. Stølen (2002), *Model-based Risk Assessment to improve Enterprise Security*, Proceeding of the 6th International Enterprise Distributed Object Computing Conference (EDOC'02), September 17-20, 2002, pp. 51-64., www.itsec.gov.cn (letöltés dátuma: 2011. szeptember 30.)

[2] A. Bajahzar, A. Baslem, A. Alqahtani (2012), *A Survey Study of the Enterprise Resource Planning System*, Advanced Computer Science Applications and Technologies (ACSAT), pp. 246-252.

[3] A. Chikán, E. Czakó, Z. Zoltayné Paprika (2002), *Vállalati versenyképesség a globalizálódó magyar gazdaságban*, Akadémiai Kiadó

[4] G. Danezis, J. Domingo-Ferrer, M. Hansen, J. H. Hoepman, D. Le Métayer, R. Tirtea, S. Schiffner (2014), *Privacy and Data Protection by Design*, ENISA

[5] T. Drake (1996), *Measuring software quality: a case study*, Computer Volume:29 , Issue: 11, IEEE Computer Society, pp. 78-87.

DOI: 10.21791/IJEMS.2016.1.17.

[6] D. I. Good (1998), *Producing secure digital information systems*, Aerospace Computer Security Applications Conference, IEEE, pp. 180-222.

[7] M. E. Porter (2006), *Versenystratégia*, Akadémiai Kiadó

[8] F. Redmill (2010), *ALARP Explored*, University of Newcastle upon Tyne: Computing Science, Computing Science, Technical Report Series, No. CS-TR-1197 http://www.scsc.org.uk/pubs/Alarp%20explored.pdf (letöltés dátuma: 2015.12.19)

[9] A. Rodriguez, E. Fernandez-Medina, M. Piattini (2007), *A BPMN Extension for the Modeling of Security Requirements in Business Processes*, IEICE TRANSACTIONS on Information and Systems, Vol.E90-D. No.4. pp.745-752.

[10] H. Roeckle, G. Schimpf, R. Weidinger (2000), *Process-oriented approach for role-finding to implement role-based security administration in a large industrial organization*, RBAC '00 Proceedings of the fifth ACM workshop on Role-based access control, pp.103-110.

[11] L. Szerb, J. Ulbert (2009), *The Examination of the Competitiveness in the Hungarian SME Sector: A Firm Level Analysis*, Acta Polytechnica Hungarica. Vol. 6. No.3. pp. 105-123.

[12] A. Tenner, I. DeToro (1998), *BPR – Vállalati folyamatok újraformálása*, Műszaki Könyvkiadó

[13] H. Turner, J. White, J. A. Camelio, C. Williams, B. Amos, R. Parker, *Bad Parts: Are Our Manufacturing Systems at Risk of Silent Cyberattacks?*, Security & Privacy, IEEE Volume:13 , Issue: 3. pp. 40-47.

[14] Z. Xiazhong (2011), *Applied analysis of a supply chain management model in the construction industry*, E -Business and E -Government (ICEE), pp. 1-4.

[15] *ISO 31000:2009,* Risk management – Principles and guidelines