KONTROLY V INFORMAČNÍCH SYSTÉMECH

Ing. Miroslava Dolejšová, Ph. D.
Univerzita Tomáše Bati ve Zlíně
Ústav informatiky a statistiky
dolejsova@fame.utb.cz

ABSTRAKT:
Evidence firemních informací je pro podnik cenným zdrojem, který je třeba chránit se stejnou důležitostí jako jeho jiné zdroje. Dojde-li v podniku ke ztrátě hmotného majetku, nepociťuje tuto ztrátu podnik tak silně jako ztrátu účetních dat. Protože si řada uživatelů neuvědomuje existenci různých rizik při používání informačního systému, nepovažuje otázku zajištění bezpečnosti dat za důležitou. Proto jim výše uvedený příspěvek může napomoci řešit uvedený problém.

KLÍČOVÁ SLOVA:
Informační systémy, rizika informačních systémů, kontroly v informačních systémech, bezpečnost dat

1. ÚVOD

Do doby, než byly zavedeny počítače ke zpracování dat, si mnoho podniků neuvědomovalo pravý význam informací. Informace do té doby nebyly pro podniky významné. V dnešní době si pouze několik manažerů může dovolit ignorovat koloběh informací v podniku.

Současné podnikatelské prostředí ovlivnila řada změn. K nejvýznamnějším změnám patří globalizace ekonomiky a v souvislosti s tím i přechod ke společnosti založené na informacích a znalostech. Nároky na zaměstnance i manažery v důsledku permanentních změn neustále narůstají. Ani oblast informatiky není žádnou výjimkou. Tyto změny se týkají také řadových účetních, asistentek ředitelů společností, obchodních zástupců i pojišťovacích poradců.

Každý z těchto pracovníků využívá určitý typ informačního systému pro svou práci. Při práci s příslušným informačním systémem může každý uživatel informačního systému způsobit chyby. Tyto chyby mohou být buď úmyslné se záměrem poškodit dobré jméno podniku nebo způsobené z nedbalosti. Oba typy chyb přinášejí pro společnost nepředstavitelné ztráty.

2. RIZIKA V INFORMAČNÍCH SYSTÉMECH

Úmyslné i záměrné chyby v informačních systémech představují pro podniky riziko. Riziko je charakterizováno jako nebezpečí, možnost škody, ztráty, nezdaru. Riziko je všudypřítomné u všech podnikových činností.

Při zaznamenávání a zpracování podnikových dat a vyhotovování podnikových výkazů může docházet k chybným výsledkům. Tyto zdánlivé chyby mohou vyvolat různé příčiny. Jednou z nich jsou chyby v počítačových programech, jiným důvodem může být nesprávný zápis dat.

Protože jsou uživatelé informačních systémů různí, často si neuvědomují existence rizik při používání informačních systémů. Jestliže účetní způsobí v účetním systému závažnou chybu a není schopen chybu napravit, budou škody pro společnost značně vysoké a nenávratné. Navíc pokud není zabezpečeno zálohování dat, jsou tyto škody daleko vyšší. Proto se v současné době zvyšují také nároky především na zlepšení úrovně znalostí informačních technologií u účetních společností.

2.1 Jaká jsou obvyklá rizika v informačních systémech?

Jak již bylo řečeno, řada řadových pracovníků společností si není vůbec vědoma existence rizik při využívání informačního systému. Někdy ani samotní uživatelé některá z těchto rizik nemohou ovlivnit. Může jít o následující typy rizik:

- Vedení firmy rozhodlo o pořízení takového hardwarového i softwarového vybavení, které nevyhovuje požadavkům pro zpracování podnikových dat.
- Nevhodné postupy při vývoji a testování systému ze strany dodavatele informačního systému
- Neodhalená selhání používaného software nebo hardware
- Ztráta nebo poškození dat během jejich zpracování
- Nespolehlivé zpracování dat
- Neodhalené chyby ve změnách souborů a databází
- Nedostatečné přidělení práv k využívání informačního systému
- Výskyt chyb v informačním systému
- Nedostatečná nápověda k informačnímu systému
- Podcenění školení uživatelů
- Nenávratné ztráty dat při výpadku elektrické energie
- Podcenění možnosti bezpečného zálohování podnikových dat

2.2 Může uživatel udělat chybu?

Odpověď na otázku je velmi jednoduchá. Chybu může udělat kdokoliv: zkušený i nezkušený uživatel. Některé chyby jsou vyvolány neúmyslně (chybný zápis dat bez následné kontroly zdrojových dokumentů), jiné chyby jsou záměrné (například zkreslování účetních dat s cílem vykázat nesprávné účetní výkazy, úmyslné nabourání se do systému s cílem zneužití dat). Protože účetní data jsou nejcennějším zdrojem informací v každém podniku, představuje ztráta těchto dat pro řadu společností mnohem vážnější problém než odcizení majetku.

Nebezpečí možného poškození nebo ztráty podnikových dat vyvolává zvýšené obavy nejen u tvůrců informačních systémů, ale především u účetních, kteří s těmito daty každodenně pracují. Tyto obavy můžeme rozdělit do tří základních skupin:

- **Havárie systému**

  Počítačový hardware, software, případně datové soubory mohou zničit požár, přerušení dodávky elektrické energie, případně jiné příčiny. Tyto poruchy nejsou úmyslné, třebaže mohou podstatně narušit běžnou činnost podniku. Může trvat řadu let než se firmě podaří obnovit zničená data a počítačové programy, pokud nemá k dispozici žádné zálohy dat. Řešením je pořízení záložního zdroje dat UPS (Uninterruptive Power Supply).

  K porušení dat může dojít i při násilném ukončení programu nebo při předčasném vypnutí počítače. Tyto chyby mohou být úmyslné i neúmyslné. Úmyslná chyba nastane právě při snaze rychle ukončit práci se systémem, aniž byly uzavřeny všechny spuštěné programy. Úmyslná chyba je to proto, že uživatel nerespektuje základní pravidla práce se systémem. Řešením v tomto případě je zavírat programy standardním způsobem a počkat na zobrazení hlášení o vypnutí počítače v případě, že není nastavena možnost jeho automatického vypnutí.

Jiné chyby představují různá chybová hlášení počítače, která nejsou způsobena uživatelem vůbec. Především při práci v síti, kdy je připojeno více uživatelů, se objevují častá hlášení o ukončení spouštěných programů. V některých případech může být chyba v počítačovém hardware, jindy v kapacitě operační paměti. Při přetížení sítě často není možné spouštět programy vůbec. Jediným řešením v tomto případě je počkat na jinou dobu, kdy nebude síť přetížena, případně pracovat prozatím s daty uloženými na lokálních discích.

- **Chyby v datech**

  Někteří uživatelé si často ani neuvědomují, že špatné zadání dat, chyby ve zpracování dat, chybné zobrazení výstupů nebo chyby při přenosu dat mohou mít pro podnik katastrofální důsledky. Především se to týká účetnictví. Řešením je permanentní kontrola vkládaných dat spolu s kontrolou původních zdrojových dokumentů, kontrola správnosti zaúčtování a spouštění kontrolních sestav.

- **Počítačová bezpečnost**

  Otázku bezpečnosti dat si mnozí uživatelé neuvědomují. Smyslem bezpečnosti je zabránit neoprávněnému přístupu k informačnímu systému, možným změnám v souborech, krádeži nebo poškození počítačového vybavení. S otázkou bezpečnosti informačních systémů je úzce spojena i počítačová kriminalita. Řešením problému počítačové bezpečnosti je návrh směrnic a opatření k lepšímu zabezpečení podnikových dat.

3. KONTROLY V INFORMAČNÍCH SYSTÉMECH

K minimalizaci chyb, počítačového selhání a počítačové kriminality musí musí podnik zavést speciální postupy. Tyto postupy by měly specifikovat způsoby ochrany majetku podniku, požadavky na přesnost a spolehlivost dat, zajištění bezpečnosti, které jsou všichni zaměstnanci podniku povinni dodržovat. Tyto postupy se označují termínem kontroly.

Kontroly můžeme rozdělit do dvou základních skupin: obecné kontroly a aplikační kontroly. Obecné kontroly slouží k ochraně informačního systému jako celku. Jsou univerzální pro všechny podnikové aplikace. Aplikační kontroly jsou kontroly, které jsou specifické pro každou konkrétní aplikaci. Jiné kontroly budou existovat v evidenci mezd a jiné v evidenci pohledávek.

3.1 Typy obecných kontrol

Cílem obecných kontrol je kontrola návrhu, bezpečnosti a využití počítačových programů a datových souborů v informačním systému jako celku. Součástí obecných kontrol mohou být tyto typy kontrol:

- Implementační kontroly

  Implementační kontroly prověřují proces vývoje informačního systému. Soustřeďují se na hledání výskytu kontrolních bodů (milníků) v etapách vývoje systému, k jakým patří například dokončení návrhu systému, návrhu specifikací, testování dat, které jsou potřebné pro schválení či neschválení dalšího procesu implementace systému. Implementační kontroly přezkoumávají i míru zapojení uživatelů v každé etapě implementace a prověřují výsledky analýzy nákladů a přínosů při posuzování realizovatelnosti systému. Součástí implementačních kontrol je kontrola technické a uživatelské dokumentace.

- Softwarové kontroly

  Softwarové kontroly sledují využívání systémového software a zabraňují neoprávněnému přístupu k systémovému software a počítačovým programům. Součástí softwarových kontrol jsou také kontroly bezpečnosti programů, jejichž cílem je zabránit neoprávněným změnám programů systému

- Hardwarové kontroly

  Cílem hardwarových kontrol je zajištění fyzického zabezpečení počítačového vybavení a kontrola jeho možného selhání. Jedná se o běžné požadavky na zabezpečení počítačového vybavení. K počítačovému vybavení má mít přístup pouze oprávněná osoba. Počítačové vybavení má být zabezpečeno proti požáru a extrémním teplotám a vlhkosti. Nezbytností je také zajistit zdroje pro zálohování dat v případě výpadku elektrické energie.

- Kontroly počítačového zpracování

  Cílem těchto kontrol je zajistit řádné a správné provádění postupů při zpracování a údržbě dat. Smyslem je odhalit chyby, ke kterým došlo při neobvyklém zpracováním podnikových dat a provést korekci těchto chyb. Po skončení zpracování lze zobrazit a vytisknout celkový průběh zpracování dat ve formě systémových žurnálů a odhalit tak možné chyby, k nimž došlo při nečekaném selhání hardwaru, nezvyklém ukončení programu, případně neobvyklé činnosti uživatelů. Můžeme také zjistit, který uživatel danou operaci prováděl a v jakém čase.

  Ke korekci chyb je třeba navrhnout specifické instrukce pro zálohování a obnovu dat, aby v případě selhání hardwaru nebo softwaru, obnově programů, systémového software a datových souborů nedošlo k chybným změnám v systému.

- Kontroly dat a bezpečnosti práce na síti

  Kontroly dat a bezpečnosti práce na síti zabraňují neoprávněnému přístupu, změnám nebo zničení podnikových dat. Jde o zavedení systému hesel ze strany administrátorů sítě a bezpečnostních profilů. Přidělená hesla jsou přidělena pouze oprávněným osobám a nikdo další se již nemůže přihlásit do systému bez platného hesla. Bezpečnostní profily umožňují administrátorům sítě nastavit typ přístupu k určitým souborům, může omezit typy dat, k nimž může uživatel přistupovat. Tímto způsobem je možné zabezpečit kontrolu práce uživatelů a sledovat na dálku, jaké činnosti provádějí, který soubor spouštějí, jaké operace se souborem provádějí, zda se nepokoušejí nabourat do systému.

3.2 Typy aplikačních kontrol

Aplikační kontroly zahrnují automatizované i manuální postupy. Účelem těchto postupů je zajistit, aby došlo ke zpracování pouze oprávněných dat, aby tato data byla zpracována úplně a přesně konkrétní aplikací. Aplikační kontroly musí vzít v úvahu celý průběh zpracování, tj. od prvotního záznamu dat až po prezentaci výstupů.

Aplikační kontroly se soustředí na následující cíle:

1. Úplnost vstupních dat a jejich aktualizace

   Všechny transakce musí být zaznamenány do počítačových souborů a musí být přístupny počítačovým zařízením

2. Přesnost vstupních dat a jejich aktualizace

   Data musí být v informačním systému přesně zaznamenána a správně zaznamenána do počítačových souborů

3. Platnost dat

   Data musí schválit oprávněná osoba s ohledem na přiměřenost transakce. Transakce musí vyjadřovat skutečný stav.

4. Údržba dat

   Data uložená v počítačových souborech musí zůstat trvale správná a aktuální.

Aplikační kontroly lze rozdělit na vstupní kontroly, kontroly zpracování a výstupní kontroly.

3.1.1 Vstupní kontroly

Smyslem vstupních kontrol je ověření dat z hlediska úplnosti a přesnosti při jejich vkládání do informačního systému. Existují specifické vstupní kontroly pro autorizaci vstupů, vstupní kontroly pro konverzi dat, editaci dat a pro manipulaci s daty.

- **Autorizace vstupů**

  Vstupní data musí být řádně schválena, zaznamenána a sledována. Je třeba však zavést postupy, aby vstupní data zaznamenávaly pouze oprávněné osoby a aby byly zavedeno řádné číslování jednotlivých dokladů.

- **Konverze dat**

  Vstupy musí být řádně převedeny do počítačových transakcí bez výskytu chyb. Chyby při převodech transakcí lze omezit nebo snížit přímým vkládáním vstupních transakcí do počítače. Pro kontrolu dat je třeba zavést kontrolu přes kontrolní součty.

- **Kontroly při editaci dat**

  Při editaci vstupních dat může docházet ke vzniku chyb před jejich vlastním zpracováním. Transakce, které nevyhovují kontrolám editace dat, jsou odmítnuty. Kontrolní postupy při editaci dat vytvářejí seznam chyb. Tyto chyby bude nutné později opravit. Mezi významné techniky pro editaci dat patří:

  Kontroly smysluplnosti: Data musí být obsažena v předem stanovených omezeních. Pokud v těchto omezeních nebudou obsažena, nebudou zpracována.

  Kontroly formátu: Systém bude kontrolovat charakteristiky obsahu (kontrola datových typů, velikosti dat, případně jiných charakteristik obsahu dat).

  Kontroly trvanlivosti: Systém porovnává vstupní data s matričními soubory (smyslem je zabezpečení správného kódování dat).

  Kontroly závislostí: Systém kontroluje, zda jsou zachovány logické vazby mezi daty stejné transakce. V případě, že tomu tak není, je transakce odmítnuta.

  Kontrolní součty: Zvláštní referenční údaj nese identifikační kód a obsahuje matematické závislosti mezi jinými kontrolními součty. Kontrolní součet se vkládá společně s daty, je pravidelně přepočítáván počítačem a výsledek je porovnáván s libovolným vstupem.

3.1.2 Kontroly zpracování

Kontroly zpracování slouží k tomu, aby data byla úplná a přesná během jejich aktualizace. K hlavním kontrolám zpracování patří kontrola celkového průběhu zpracování, počítačové porovnání a programové kontroly editace.

Kontrola celkového průběhu zpracování srovnává součty vstupních kontrol se součty aktualizovaných položek. Výsledky porovnání jsou zaznamenány pro další zkoumání.

Počítačové porovnání porovnává vstupní data s informacemi obsaženými v matričních nebo dočasných souborech. Neporovnané položky jsou zaznamenány pro další zkoumání. K většině srovnání dochází během zápisu vstupních dat, ale za určitých okolností může být toto porovnání vyžadováno k zajištění úplnosti aktualizace.

Programové kontroly editace ověřují smysluplnost nebo konzistenci dat. Většina těchto typů kontrol probíhá při zápisu vstupních dat. Přesto některé aplikace mohou také vyžadovat určitý typ kontroly smysluplnosti nebo trvanlivosti během aktualizace.

3.1.3 Výstupní kontroly

Výstupní kontroly zajišťují, aby výstupy počítačového zpracování byly přesné, úplné a byly řádně distribuovány. Obvyklé výstupní kontroly jsou následující:

- Porovnání výstupních součtů se vstupními součty nebo součty v průběhu zpracování
- Přezkoumání záznamů týkajících se zpracování dat (účelem je kontrola řádného zpracování všech dat)
- Prověření výstupních dokumentů (účelem je zajistit správnost součtů, formátů, případně jiných informací a jejich soulad se vstupními kontrolními součty)
- Formální postupy specifikující oprávněné příjemce výstupů

4. CO MOHOU PODNIKY UČINIT PRO LEPŠÍ ZABEZPEČENÍ SVÝCH DAT?

Mají podniky nějaké možnosti, jak si lépe zabezpečit svá data? Existuje několik možností:

a) Definování přístupových práv

Každý uživatel má přiděleno od svého administrátora své uživatelské jméno a heslo. Tak nebudou moci se stejnými záznamy pracovat různí zaměstnanci podniku. Přidělená hesla není vhodné sdělovat jiným osobám. Je také žádoucí hesla pravidelně měnit.

b) Zabezpečení firemních databází

Smyslem zabezpečení firemních databází je jejich ochrana před neoprávněným přístupem. Uživatelé si mohou zabezpečit ochranu podnikových dat zadáním interního hesla. Toto heslo může být také vyžadováno při importu dat. Zabezpečení databází je možné kdykoliv zrušit.

c) Uzamčení firemních záznamů

Uživatel může uzamknout pouze jeden konkrétní záznam, uzamknout vybrané záznamy nebo uzamknout všechny záznamy. Smyslem uzamčení záznamů je ochrana před nežádoucími úpravami dat.

d) Zálohování dat

Je naprosto nezbytné pravidelné zálohování dat. Při výpadku elektrického proudu nebo při chybách v počítačovém programu může jedině záloha zachránit podniková data. V opačném případě budeme nuceni všechny chybějící záznamy zavádět znovu. Zálohování musí uživatelé provádět denně.

Neméně důležitou povinností je používání bezpečných médií. Diskety nejsou spolehlivými médii a jejich kapacita je malá. Vhodnější je zálohovat na záložní pevný disk, výměnný disk, případně vypálit účetní data na disky CD-RW.

Zálohy by měli uživatelé ukládat na bezpečná místa, pokud možno ve více kopiích. Může dojít k situaci, kdy záloha bude poškozena, dojde ke krádeži počítače, případně ke špatnému zálohování dat. Z tohoto důvodu má uživatel k dispozici více kopií stejné zálohy dat. Poslední zálohu je třeba občas vyzkoušet, zda není poškozena.

V případě, že uživatel nemůže otevřít počítačový program, musí načíst data ze záložní kopie. Je třeba uživatele upozornit na to, že stávající data budou záložní kopií automaticky přepsána.

e) Správa a údržba firemních databází

Správa a údržba firemních databází umožňuje provádět automatické zálohování podnikových dat, kontrolovat, opravovat a komprimovat strukturu firemní databáze. Při porušení firemní databáze lze uložená data zachránit.

Jinou možností údržby je obnova firemní databáze. Obnova firemní databáze probíhá tak, že se vytvoří nová struktura databáze a převedou se na ni data z porušené databáze. V případě, že je obnova databáze úspěšná, jsou data zachráněna. V opačném případě může uživatel načíst účetní data z poslední zálohy.

Součástí správy a údržby databáze je i oprava integrity dat. Opravy integrity dat jsou nezbytné zejména po výpadku elektrické sítě, pádu aplikace nebo systému Windows. Obvykle se ochrana integrity dat používá při vedení skladových zásob. Po spuštění této funkce dochází k automatickému přepočtu stavu zásob na skladě, přepočtům nákupních cen a aktualizacím pohybů zásob.

V době, kdy s počítačovým programem uživatel nepracuje (obvykle přes noc), je vhodné provést automatickou údržbu databáze.

f) Používání záložního zdroje UPS při výpadku elektrického proudu

Záložní zdroj UPS (Uninterruptive Power Supply) pro napájení počítače je velmi důležitý. Jeho hlavní význam spočívá v ukládání dat při možných poruchách počítače, aby nedošlo ke ztrátě nebo porušení dat. K porušení dat může dojít i při násilném ukončení programu pomocí tzv. teplého startu nebo při předčasném vypnutí počítače. Řešením je zavírat programy standardním způsobem a počkat na zobrazení hlášení o vypnutí počítače v případě, že není nastavena možnost jeho automatického vypnutí.

5. BEZPEČNOST NA INTERNETU A ÚČETNICTVÍ

Pokud má firma zřízeno internetové bankovnictví, vystavuje se ještě větším rizikům. Třebaže se firma přihlašuje k internetovému bankovnictví formou hesla, nemusí to ještě znamenat, že o svá data nemůže přijít. Informace nemusí být jenom vymazány, někdo je firmě může ukrást. Z tohoto důvodu každá firma potřebuje mít základní ochranné prostředky pro bezpečnou ochranu svých dat i na Internetu.

a) používání antivirových programů

Nejčastějšími příčinou nefunkčnosti počítačových programů jsou viry. Pokud je počítač virem napaden, může zničit velmi cenná data a napáchat nepředvídatelné škody. Nainstalovaná antivirová aplikace je pro počítač připojený k Internetu naprostou nutností. Moderní antivirové programy jsou schopny dostatečně chránit před klasickými viry i červy a k jejich aktualizaci dochází obvykle do několika hodin po objevení nové hrozby. Čas od času je vhodné provádět kompletní test celého počítače. K nejpoužívanějším českým antivirovým programům patří systémy AVG Antiviru (www.avg.cz) a Avast! (www.asw.cz).

b) používání firewallů

Antivirový program ochrání firmu před viry a před červy. Neochrání ji například před možným útokem, před pokusem o zneužití bezpečnostní mezery v operačním systému, které by mohly způsobovat potíže se sítí, případně vykrádat firemní data. Právě před tím nás ochrání firewall. K nejznámějším firewallům patří produkty Zone Alarm firmy Zone Labs (www.zonealarm.cz) a Kerio Personal Firewall (www.kerio.cz).

c) používání spyware

Spywarové komponenty jsou aplikace, které monitorují chování uživatele a na jeho základě mu servírují reklamu. Spyware sice přímo nepoškozuje počítač, poškozuje spíše uživatele systému. Aplikace běžící na pozadí mají schopnost prakticky vykrádat data, parazitovat na prostředcích počítače, jeho paměti i na internetovém připojení. V každém případě znamenají vážné ohrožení bezpečnosti dat. K ochraně před spyware existují dvě kvalitní aplikace: komerční Ad Avare (www.lavasoft.de) a amatérský Spybot Search & Destroy

(www.security.kolla.de). Obě aplikace mají schopnost aktualizace prostřednictvím Internetu podobně jako antivirové programy.

d) šifrování dat

Velmi účinný prostředek pro zabezpečení dat především při přenášení elektronických dat. Jde o transformaci dat do nečitelné podoby. Důvodem pro šifrování je ochránit důvěrné a osobní informace znemožněním jejich čitelnosti pro všechny, komu nejsou určeny, dokonce i pro osoby, které mají přístup k těmto šifrovaným datům. Šifrování vyžaduje užití nějaké tajné informace obvykle označované jako klíč. Tento klíč obsahuje řetězec alfanumerických znaků. Jakmile jsou data šifrována, mohou být bezpečně uložena na nedostatečně chráněných médiích nebo přenášena po nechráněných sítích (Internet)

6. ZÁVĚR

Většina podniků již pochopila, že informace jsou jejich významným zdrojem. Současné organizace si nemohou dovolit, aby docházelo ke ztrátám informací. Dnešní doba nutí podniky, aby využívaly příležitostí, které se jim naskytnou, a aby co nejrychleji reagovaly na různá ohrožení. Pouze firmy, které jsou schopny čelit těmto rizikům, mají šanci dosáhnout významných úspěchů.

LITERATURA

Stair, R. M.; Reynolds, G. W.: Principles of information systems: a managerial approach. Thomson/Course Technology, Boston, USA, 2003. ISBN 0-619-06489-7.