Monitorovanie pracovných staníc v komerčnom sektore

Jaroslav Oster
Info consult, s.r.o.
Martina Rázusa 29
984 01 Lučenec
e-mail: oster@slovanet.sk

Abstrakt

Otázka kde je hranica medzi elektronickym súkromím zamestnanca a ochranou záujmov zamestnávateľa je značne citlivou témou. Zneužívanie aktív zamestnávateľov na súkromné účely od najnevinnejších foriem až po „beznákladové“ podnikateľské aktivity pri ktorých znáša náklady zamestnávateľ, nárast počtu prípadov internej IT kriminality s často vážnymi dopadmi na funkčnosť i prestíž firiem vytvárajú priestor na rozsiahlu diskusiu o tejto téme. Je monitorovanie „prenasledovaním“ zamestnanca alebo multifunkčným nástrojom zabezpečujúcim spätnú väzbu personálnej, bezpečnostno-preventívnej a rozpočtovej politiky komerčných subjektov?

The question of a dividing line between employee's electronic privacy and the protection of his employer's interests is quite a sensitive topic. Various misuses of employers' assets for private intents - ranging from the most innocent forms to forms of "free of expenses" buisness activities (in which employers bear all charges) or an increase in internal IT criminality with serious consequences on functionality and prestige of corporations create space for some vast discussion on the topic. Is monitoring of employees an act of persecution or is it a multifunctional tool that provides a feedback for personal, safety and preventive and fiscal policies of commercial entities?

1. Úvod

Informačné technológie dnes patria k neodmysliteľným pracovným nástrojom. Bez počítačov, softvéru, tlačiarní a ďalších prvkov, ktoré združujeme pod pojem informačno-komunikačné technológie (IKT) sa dnes nazaobíde pravdepodobne žiadna komerčná spoločnosť .

Budovanie IKT v prostredí samosprávy tak ako vo všetkých oblastiach spoločnosti prešlo rôznymi vývojovými štádiami – počnúc budovaním technologickej infraštruktúry, riešením softvérového vybavenia, edukáciou používateľov v základných používateľských znalostiach a zručnostiach, budovaním databázových systémov až po súčasnú dobu, kedy sa manažmenty začínajú orientovať v problematike prevádzkovania IKT z hľadiska rizík i z hľadiska ich efektívneho využívania. Aplikovateľnosť IKT má neustále narastajúcu tendenciu, čo úplne logicky bude klásť zvýšené nároky na všetky aspekty prevádzky. Prevádzkovanie informačných technológií je často považované za „čiernu dieru“. Nie je ojedinelým názor vnímania IT systémov ako nutného zla – prostriedku bez ktorého sa síce ťažko

zaobísť, ale na jeho prevádzku je nutné vynakladať značné finančné prostriedky. Úplne logicky v takejto situácií vzniká rad otázok na ktoré ekonomicky zmýšľajúci manažment prirodzene hľadá adekvátne jednoznačné odpovede smerujúce k myšlienke „ako vybudovať spätnú väzbu umožňujúcu zaviesť poriadok“

2. Používateľ informačného systému ako rizikový prvok

Zamestnanec (externý alebo interný) využívajúci prostriedky IKT v pozícii oprávneného používateľ pri zabezpečovaní svojich pracovných činností vyplývajúcich z jeho pracovného zaradenia predstavuje v téme bezpečnej a efektívnej prevádzky IKT istý rizikový faktor.

Pokúsme sa na túto otázku pozrieť z dvoch základných uhlov pohľadu:

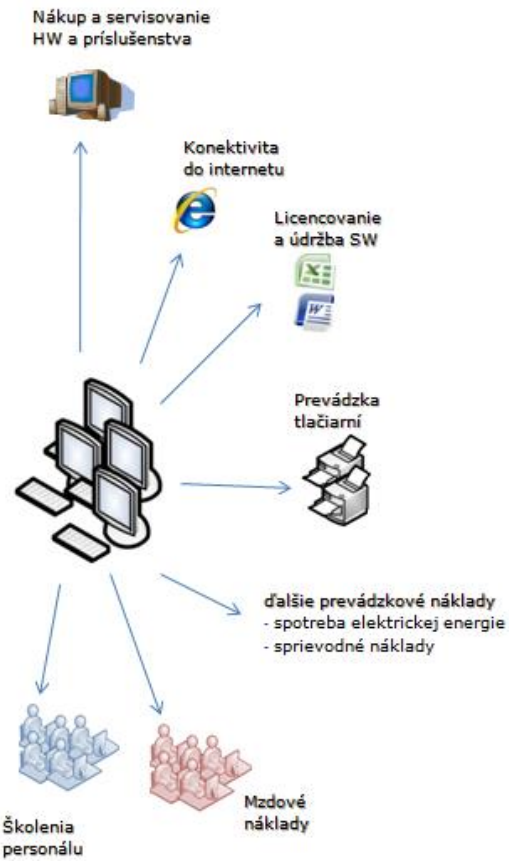
1. z pohľadu nežiadúcich nákladov, ktoré musí zamestnávateľ t.j. prevádzkovateľ IKT vynakladať na prevádzku nad rámec nutných nákladov potrebných pre zabezpečenie komerčných cieľov
2. z pohľadu bezpečnosti IKT

2.1. Zamestnanec versus náklady na prevádzku IKT

IKT prevádzkovateľ (je principiálne jedno či vo firemnom alebo samosprávnom prostredí) zriaďuje a prevádzkuje obykle pre účely poskytnutia pracovného prostriedku pre svojich zamestnancov – teda pre účely výkonu pracovných povinností. Aká je však realita?

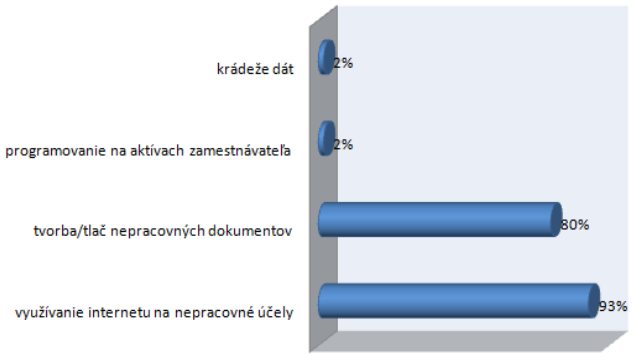
Prevádzkovatelia IKT nie raz riešia elementárne otázky súvisiace s nákladovosťou na ktoré nie je jednoduché dáť jednoznačné odpovede, spomeňme len niektoré priamo z praxe:

- aká je efektivita investícií do rozvoja IT infraštruktúry
  - nákup počítačov, notebookov a periférií
  - nákup nových licencií softvérového vybavenia
  - nákup služieb pre podporu prevádzky SW vybavenia
  - nákup update a upgrade
- nie je možné ušetriť presunutím HW na iné pracoviská?
- nie je možné ušetriť presunutím SW licencií?
- prečo sa zahlcuje sieť (dáta idú von alebo dnu/sú to cielene posielané dáta alebo ide o mallware)?
- kto sťahuje tie obrovské množstvá dát (ide o neškodné dáta/SW pirátstvo/protizákonné dáta?)
- pracuje sa na počítačoch alebo sa hrajú hry?
- kam mizne toľko papiera a náplní do tlačiarní?
- prečo sa zaplňujú lokálne disky (SW/mpeg/mp3)?

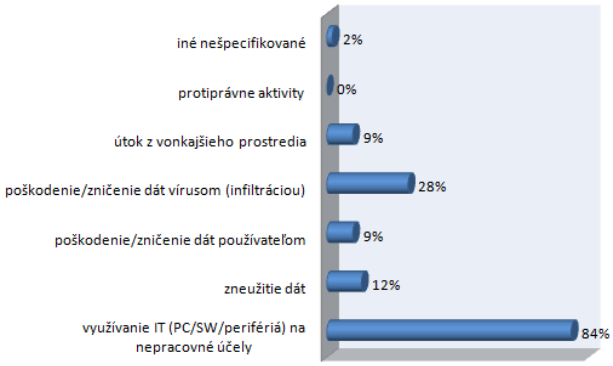


Obrázok 1: Náklady prevádzkovania IKT

Prieskumy a rovnako aj praktické skúsenosti manažmentov, správcov systémov i konzultantov však poukazujú, že v oblasti pracovnej disciplíny pri využívaní počítačovej techniky sú návyky zamestnancov značne deformované a z hľadiska zamestnávateľov často nežiadúce návyky. Pre ilustráciu prieskum realizovaný v roku 2011 do ktorého sa odpoveďami zapojilo celkom 46 mestských úradov Slovenskej republiky



Najčastejšie identifikované formy využívania IKT na nepracovné účely (zdroj: *„Prieskum SAMOSPRAVA 2011, Info consult“)*

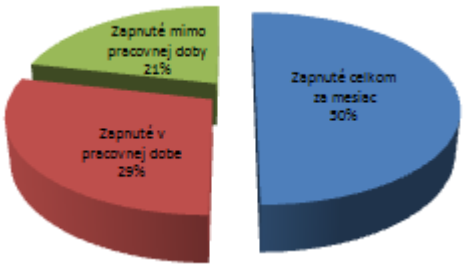


Najčastejšie identifikované formy rizík využívania IKT (zdroj: *„Prieskum SAMOSPRAVA 2011, Info*

Zaujímavé pohľady na tému nákladov pri prevádzke IKT vynakladaných nad rámec nutných výdavkov na prevádzku priniesli prieskumy zo sektoru SMB firiem publikované v predchádzajúcom kalendárnom roku:

- vo firmách SMB sektoru sa vytlačí takmer 1/3 tlačených strán zbytočne – podstatnú časť z toho tvorí tlač nepracovných dát (*zdroj: prieskum SODATSW Brno, 2011*)

- zamestnanci nechávajú počítače bezdôvodne zapnuté často aj v mimopracovnej dobe a to v priemere až 120 hodín mesačne (*zdroj: prieskum SODATSW Brno, 2011*)



- zneužívanie firemného internetu zamestnancami na nepracovné účely registruje viac ako dve tretiny slovenských podnikov *(zdroj: prieskum GFI, 2011)*

- pomer času stráveného pracovnými a nepracovnými aktivitami súvisaicimi s využívaním internetu je 480 minút k 80, čo takmer 17% pracovného fondu (*zdroj: prieskum SODATSW Brno, 2011*)

- väčšina zverejňovaných prieskumov sa zhoduje v poznaní, že 30-40% aktivít na internete nesúvisí s pracovnými aktivitami

Využívanie prostriedkov výpočtovej techniky zamestnávateľa na súkromné účely sa stali úplne rozšírenou a žiaľ často v prehnanej miere tolerovanou formou pracovného správania zamestnancov. Pritom zavedenie poriadku môže priniesť nemalú úsporu zbytočne vynaložených nákladov.

2.2. Zamestnanec ako rizikový faktor

Nedisciplinovaný zamestnanec neakceptujúci základné požiadavky kladené na jeho prácu s IKT predstavuje aj zásadný bezpečnostný rizikový faktor, Súčasným problematickým javom s narastajúcou tendenciou sa v internom prostredí stáva narastajúci počet prípadov rizikového správania používateľa zasahujúcich do roviny trestného práva. Manažmenty sú čoraz častejšie konfrontované s problémom využívania svojich aktív na páchanie trestnej činnosti zo strany zamestnanca/ov.

Niekoľko zobecnených príkladov rôznej závažnosti nesúcich riziko nie len neefektívneho využívania počítačov, ale aj vážneho poškodenia povesti prevádzkovateľa, či ďalších nepríjemných následkov:

- využívanie prostriedkov IT na súkromné (nepracovné aktivity)
  - surfovanie po internete nesúvisiace s pracovnými úlohami
  - tlač nepracovných dát
  - napaľovanie/duplikácia médií
  - využívanie strojového času zamestnávateľa na programovanie
  - a ďalšie
- sťahovanie/šírenie dát podliehajúcich autorskoprávnej ochrane – SW/film/hudba...
- sťahovanie/šírenie dát nemorálneho alebo protizákonného charakteru – xenofóbia,rasizmus, detská pornografia,...
- vytváranie neautentických dát s cieľom vydávať tieto za autentické – dokumenty pre páchanie podvodov ekonomického charakteru (daňové, poisťovacie, dotačné a rôzne ďalšie)
- poškodzovanie záujmov zamestnávateľa rôznymi formami
  - zapájanie sa do rôznych diskusií nepracovného charakteru spojené s nejednoznačným oddelením identity diskutujúceho od zamestnávateľa (názor pôsobí ako oficiálne stanovisko)
  - zneužívanie internetovej konektivity zamestnávateľa na maskovanie identity pri zverejňovaní príspevkov na chatových portáloch – najmä príspevky charakteru ohovárania, zverejňovania privátnych kompromitujúcich fotografií a videozáznamov, klamlivých inzerátov,
  - sprístupňovanie dôverných dát na diskusných fórach – napríklad informácie tvoriace obchodné tajomstvo zamestnávateľa, operatívne informácie
- krádeže dát zamestnávateľa za účelom získania výhody
  - pre svoje podnikateľské aktivity
  - pre potreby konkurencie
- iné zámerné aktivity smerujúce k narušeniu dôvernosti, dostupnosti, integrity dát s cieľom poškodiť zamestnávateľa

Zaujímavým z tohto pohľadu je ignorovanie javov ktoré v kombinácii s rizikom zo strany používateľa predstavuje nekontrolovaný pohyb pamäťových zariadení v prostredí firiem. Značné percento prevádzkovateľov IKT dnes priznáva, že pohyb USB zariadení použiteľných ako úložisko a teda možný kanál úniku citlivých dát zo spoločnosti nemajú pod kontrolou.

3. Východisko – spätná väzba

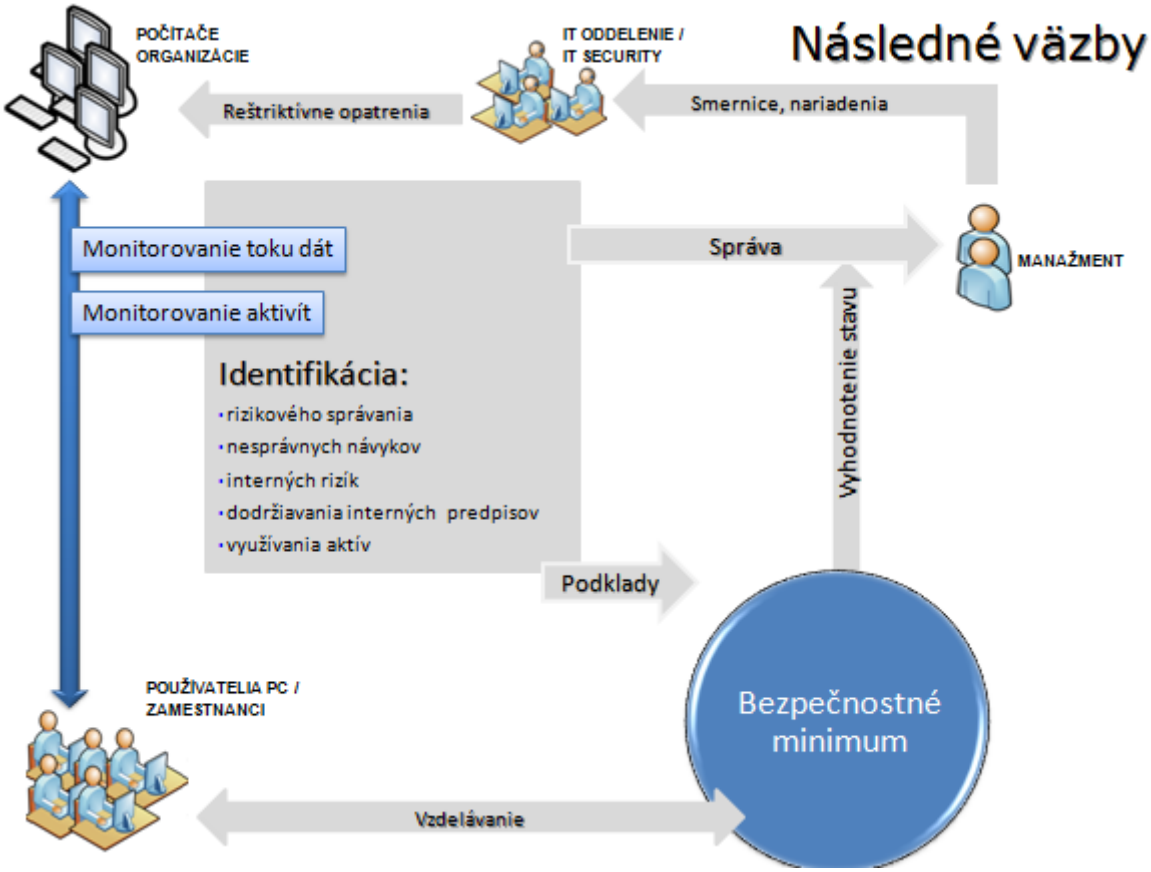
Princíp ako tento problém vyriešiť je veľmi jednoduchý a je možné ho zhrnúť do 3 bodov:

1. zaviesť jasné pravidlá s jasne vymedzenými požiadavkami voči zamestnancom - používateľom
2. tieto pravidlá vhodnou formou odkomunikovať so zamestnancami , pričom ideálne je vytvoriť cyklický proces vzdelávania zameraný práve na problematiku bezpečného a efektívneho prevádzkovania informačných technológií
3. zaviesť systém spätnej kontroly – nasadením vhodného technologického riešenia realizovať systém operatívnej kontroly (monitorovania) využívania aktív

3.1. Monitorovanie

Vyššie uvedené argumenty sú dostatočné na to, aby sme mohli tvrdiť že monitorovanie pracovných staníc prevádzkovaných z finančných prostriedkov zamestnávateľského subjektu má svoje praktické a pragmatické opodstatnenie. Čo však môžeme konštatovať je skutočnosť, že názory na tému právnej stránky monitorovania z hľadiska práva na súkromie zamestnanca konfrontované s právami zamestnávateľa sa dnes rôznia a stoja proti sebe dva názorové prúdy – názorová platforma presadzujúca absolútne právo na súkromie zamestnanca a názorová platforma preferujúca absolútne práva zamestnávateľa. Legislatívne ošetrenie stavu a to najmä v téme monitorovania služobnej elektronickej pošty má v súčasnom stave do dokonalosti ďaleko a určite bude vyžadovať zavedenie jednoznačne definovanej právnej normy ošetrujúcej kontrolu zamestnanca a jeho aktivít v pracovno-právnom vzťahu. Diskusie z odborných seminárov a konferencií vznesených zástupcami jednej i druhej skupiny názorov, ktoré môžu byť zaujímavým impulzom na diskusie pri ďalšom vývoji legislatívnej stránky.

Častým problém je snaha zavádzať „utajené“ formy monitorovania bez oboznámenia dotknutých zamestnancov so zavedením tejto formy kontroly. Zaviesť akýsi „bič“ použiteľný vždy v situáciách „keď je to potrebné“. V prvom rade je nutné zdôrazniť, že pri súčasne platnej legislatívnej úprave SR je táto forma neakceptovateľná. V druhom rade sa tým autori takýchto myšlienok v celom procese ochudobňujú o okamžitý prínos zavedenia takéhoto procesu – preventívny účinok. Praktické skúsenosti poukazujú, že už len vydanie smernice informujúcej o zavedení takejto formy kontroly využívania IKT zo dňa na deň mení správanie časti používateľov – z praktických skúseností konzultanta môžem potvrdiť okamžité a rapídne (identifikovateľné a merateľné) zníženie návštevnosti pornografických stránok a zníženie objemu downloadu z rôznych internetových serverov.



Praktické prínosy zavedenia monitoringu a na nadviazateľných činností

Operatívne

- ✓ jednoznačný a prehľadný monitoring využiteľnosti PC
- ✓ zadefinovanie a zahájenie procesu edukácie v oblasti bezpečnosti IKT
- ✓ pochopenie nutnosti existencie bezpečnostných opatrení aplikovaných vnútornou smernicou zo strany zamestnancov
- ✓ odkomunikovanie základných rizík a protiopatrení voči týmto rizikám v prostredí zamestnávateľa
- ✓ zvýšenie bezpečnostného povedomia používateľov IKT

Dlhodobé prínosy

- ✓ zvýšenie zodpovednosti zamestnancov pri využívaní prostriedkov IKT a spoluzodpovednosti pri presadzovaní zásad bezpečnosti
- ✓ zvýšenie bezpečnosti informačného systému
- ✓ zvýšenie pracovnej disciplíny minimalizáciou nežiadúcich foriem využívania IKT na nepracovné účely
- ✓ využiteľnosť operatívnych poznatkov pre riadenie licenčnej politiky, investícii do rozvoja IKT, riadenia prevádzových nákladov, personálneho riadenia aj ako nástroja aktívnej prevencie internej IT kriminality

4. Záver

Už len zavedenie opatrení ako je monitorovanie pracovných staníc má silný preventívny účinok, prax jednoznačne preukazuje že už pri prvotnom spustení procesu a správnom odkomunikovaní sa mení postoj zamestnancov k otázke využívania aktív zamestnávateľa. Strata pocitu bezbrehej a nekontrolovateľnej anonymity vnáša do pracovnej disciplíny nový rozmer, ktorý prirodzene prináša zvýšenie efektivity a rovnako aj bezpečnosti využívania informačných systémov.

Ak manažmenty komerčných firiem dokážu nájsť vhodnú formu ako tento proces monitorovania zaviesť do reálnej praxe fungovania firmy kedy nebude vnímaný ako nástroj „prenasledovania“ zamestnanca a dokážu získané výstupy prepojiť s ďalšími procesmi získajú v riadiacej práci silného pomocníka. Získajú multifunkčný nástroj zabezpečujúcim spätnú väzbu personálnej, bezpečnostno-preventívnej a rozpočtovej politiky pomáhajúci riešiť medziiným aj zásadnú otázku dnešných dní – otázku ako a kde znižovať náklady na prevádzku a súbežne s tým zvyšovať bezpečnosť.

Literatúra

[1] Jaroslav Oster: *prednáška IT kriminalita v internom prostredí prevencia a represia, konferencia,* zborník konferencie Zmluvy v IT,eFocus 2011

[2] Jaroslav Oster: *prednáška Čo majú spoločné neidentifikované náklady na prevádzku IT, rizikové správanie používateľa IT a zlá licenčná politika,* zborník konferencie Nemocničné informačné systémy, 2011

[3] Info consult: *Prieskum Samospráva 2011*

[4] SODATSW Brno: *Prieskum SMB,* 2011