

UDK: 004

Stručni rad

UTICAJ LJUDSKOG FAKTORA U PRIMENI INFORMACIONIH TEHNOLOGIJA NA PRIMERU IS ZU “APOTEKA VRANJE”

EFFECT OF HUMAN FACTORS IN THE USE OF INFORMATION TECHNOLOGY FOR THE EXAMPLE IS ZU "APOTEKA VRANJE"

Irena Tasić¹

¹ Visoka škola akademskih studija “Dositej” u Beogradu

¹irena.tasic@mts.rs

Apstrakt: S obzirom na značaj delatnosti Zdravstvene ustanove “Apoteka Vranje” (AV) u Vranju javila se potreba implementacija savremenog informacionog sistema (IS) koji će biti u stanju da podrži sve poslovne funkcije AV i koji će značajno olakšati rad. AV odlučila se za uvođenje savremenog Poslovno informacionog sistema (PIS) “Hubie” koji se već koristi u ZU Apoteka Beograd i koji je osvojio prvu nagradu JISA-DISKOLOBOS kao najbolje informatičko rešenje u kategoriji Zdravstva. Ovaj IS je donacija Norveške i bio je deo pilot projekta uvođenja IS u distribuciji lekova u Srbiji. Sigurnost PIS “Hubie” može biti ugrožena na više načina, kako spolja tako i iznutra. Statistički podaci pokazuju da ugrožavanje sigurnosti najčešće prouzrokuju ljudske greške. Potraga za najadekvatnijim rešenjem dodatne zaštite od “ljudskog faktora” rezultirala je razmišljanjima o potrebi uvođenja sigurnosne politike u AV.

Ključne reči: informacioni sistem, zaštita, sigurnost, sigurnosna politika

Abstract: Regarding the importance of the business of the Pharmacy Institution (PhI) in Vranje, the necessity to implement a contemporary Information System (IS), able to support all the business activities of the PhI and make their work much easier, appeared. The PhI decided to introduce the contemporary business information system “Hubie ERP” which had already been used by the Pharmacy Institution in Belgrade and had been awarded the first prize JISA-DISKOLOBOS as the best information solution in the category of. This information system is a donation by the Norwegian government related to the introduction of an information system for the distribution of medicine in Serbia. The safety of the BIS Hubie ERP may be jeopardised in many ways, both internally and externally. Statistic data prove that the human factor is the cause of safety problems. While searching for adequate protection solutions the issue of the “human factor” was raised which brought about the necessity to think of the implementation of a safety policy in the PhI in Vranje.

Key words: Information System, protection, safety, safety policy

1. UVOD

Primena informacionih tehnologija u svakodnevnom životu dovela je do masovnog korišćenja raznih informacionih sistema (IS) u svim segmentima poslovanja. Motivacija ovog istraživanja je potreba za sve jačom sigurnošću IS. Ljudi su olakšali svoj život zahvaljujući razvoju računara i softvera. Naime, mnoge poslove koje je do pojave računara obavljao čovek, sada obavljaju i kontrolišu računari. Međutim, korišćenje IS u obavljanju svakodnevnih poslova ima i neke loše strane. Najveći problem današnjice vezan za IS je upravo sigurnost samog IS.

AV obavlja farmaceutsku zdravstvenu delatnost na teritoriji Pčinjskog upravnog okruga, u skladu sa uredbom o planu mreže zdravstvenih ustanova Ministarstva zdravlja Vlade Republike Srbije. S obzirom na važnost delatnosti i obim rada AV, cilj je bio implementirati savremen IS koji će biti u stanju da podrži sve poslovne funkcije AV i koji će značajno olakšati rad kako unutar same ustanove tako i sa sveukupnim okruženjem.

IS ne može se u potpunosti zaštititi i to je činjenica koje mora biti svestan svaki korisnik. Radnje odgovornih osoba u cilju povećanja sigurnosti sistema vrlo su individualne zbog individualnosti samih IS i stoga se ne mogu definisati univerzalne radnje prema kojima bi se gradila sigurnost sistema.

Tražeci adekvatna rešenja razvijene su mnoge danas poznate metode zaštite ali je zanemarena jedna bitna činjenica, a to je ljudski faktor. Treba napomenuti da se pod sigurnošću sistema smatra mera subjektivnog osećanja ili ubedenja da je sistem bezbedan, da mu ne pretili nikakva opasnost jer je zaštićen (osiguran) i veruje se da je mala verovatnoća negativnih faktora rizika; u semantičkom značenju to je sinonim za bezbednost sistema.

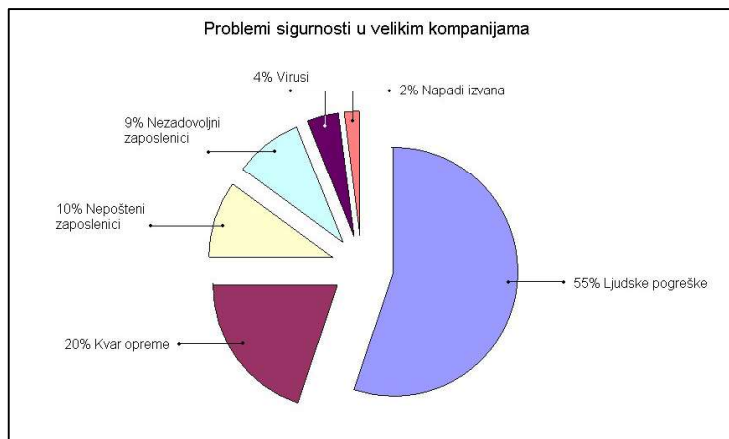
2. MATERIJALI I METODE

Za potrebe ovog rada korišćene su statističke metode u etapama. U procesu istraživanja *prva etapa* primene statističke opštenaučne metode, u skladu sa njenim pravilima i procedurom primene, jeste *identifikacija statističke mase*. Uzorkovanje i izrada uzorka čine *drugu etapu* primene statističke metode dok je *treća etapa* prikupljanje podataka. *Četvrtu etapu* u primeni ove metode čini *formiranje statističkih serija*. Formiranje serije podataka spada u fazu sređivanja i obrade podataka. *Peta etapa* jeste *statistička analiza*. Statističke podatke smo sredili u statičke serije i analizirali ih kako bi otkrili strukturu, međusobne uticaje činilaca strukture i dinamiku odigravanja istraživanih pojava odnosno procesa. *Šesta etapa* jeste *tumačenje rezultata statističke analize i izvođenje zaključaka*. Osnovni zadatak nam je bio izvođenje direktnih i indirektnih generalizacija manjeg ili većeg stepena istinitosti odnosno verovatnoće o pouzdanosti informacija o predmetu. Poslednja, *sedma faza* u primeni opštenaučne statističke metode jeste konstatovanje određenih pravilnosti u procesima koji su vezani

za procenu uticaj ljudskog faktora kao rizika po bezbednost informacionog sistema ZU Apoteka Vranje.

3. REZULTATI I DISKUSIJA

Sigurnost IS može biti ugrožena na više načina. Iako mnogi smatraju da pretnje sigurnosti IS najčešće dolaze spolja, istraživanja koja su obavljena i objavljena u knjizi D. Seger, K. VonStroch, W. "Computer Crime A Crimefighter's Handbook", O'Reilly & Associates pokazuju sasvim suprotne činjenice. Statistički podaci koji su prikazani na slici br. 1. pokazuju da u najvećem procentu problem sigurnosti prouzrokuju ljudski faktor u procentu od čak 55%.



Slika br. 1 : Problemi sigurnosti u velikim kompanijama [2]

Polazeći od činjenica da je najveći problem u bezbednosti IS upravo ljudski faktor, AV je posvetila posebnu pažnju na korisnike sistema i njihovo upravljanje računarima. Iz tog razloga je izvršena kontrola računara u AV sa ciljem otklanjanja eventualnih propusta u IS.

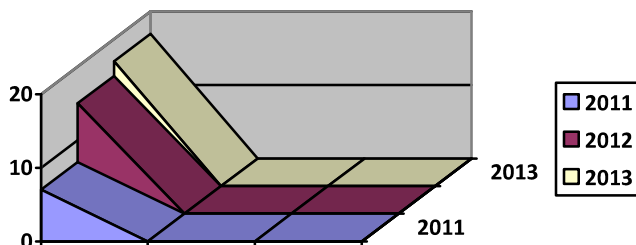
Zaposleni svojim postupcima bitno utiču na sigurnost sistema. Budući da je mogućnost njihovog uticaja na sigurnost sistema vrlo široka, važno je detaljno proučiti i predvideti na koji način oni mogu ugroziti sistem. Kako bi sistem bio kvalitetno zaštićen potrebno je uočiti sve načine na koji zaposleni može štetno delovati na sistem. U konkretnom slučaju, načini na koji zaposleni može ugroziti sistem je da zaposleni može preko Interneta, elektronske pošte ili unosom na bilo koji drugi način malicioznih programa ugroziti sigurnost sistema. Budući da zaposlenima pristup Internetu za obavljanje poslova nije potreban, treba onemogućiti njegovo korišćenje.

Kontrolisano je 80 računara ZU Apoteka Vranje i to u godinama 2011, 2012 i 2013 i došlo se do sledećih rezultata:

Tabela 1. Rezultati kontrole računara po godinama

RB	Godina	Broj „problematičnih“ računara	Procentualni iznos u odnosu na ukupan broj (%)
1	2011	7	8,75
2	2012	15	18,75
3	2013	17	21,25

“Problematičnim računarima” smatraju se računari koji su bez dozvole pristupali Internetu i koje su korisnici koristili za lične potrebe narušavajući time bezbednost celog IS. Iz grafikona se jasno vidi da je iz godine u godinu rastao broj takvih računara.




Slika 2. Grafički prikaz „problematičnih računara“ po godinama

4. ZAKLJUČAK

Pored toga što Apoteka Vranje zapošljava relativno mali broj zaposlenih koji su u direktnom kontaktu sa IS, nesporno je da su integritet i tajnost podataka u ovom slučaju vrlo važni. Gubitkom podataka Apoteka Vranje bi bila suočena sa mnogim problemima. Morala bi formirati novu bazu podataka i suočiti se sa ostalim problemima koji bi prouzrokovati velike materijalne štete.

Bilo kakva neželjena izmena podataka takođe bi dovela do velikih problema. Zbog navedenih razloga vrlo je važno preventivno delovati u smislu sigurnosti sistema. Iz tog

razloga administrator IS ZU Apoteka Vranje dužan je da svakom zaposlenom i korisniku sistema omogućiti pristup dokumentu sigurnosne politike objavljivanjem dokumenta na službenim Internet stranicama ustanove i/ili deljenjem štampanih dokumenta u javnim prostorijama ustanove. Administrator je takođe dužan dati na znanje svim zaposlenima i korisnicima sistema da sigurnosna politika ustanove postoji, tj. da je uvedena. Osim toga neophodno je izraditi *Pravilnik o primeni informacionih tehnologija u ZU Apoteka Vranje* kojim bi se definisala prava i obaveze zaposlenih uz obavezno potpisivanje izjave o prihvatanju pravila i uslova iz navedenog Pravilnika.

	ZU APOTEKA VRANJE DIREKCIJA: Objekat: Broj:										
	<p>Na osnovu člana 17. Pravilnika o primeni informacionih tehnologija u Zdravstvenoj ustanovi Apoteka Vranje, (u daljem tekstu: ZU Apoteka Vranje), zaposleni daje sledeću</p> <p style="text-align: center;">I Z J A V U</p> <p>Pročitao sam, razumeo, i prihvatom pravila i uslove iz „Pravilnika o primeni informacionih tehnologija“ ZU Apoteka Vranje koji reguliše korišćenje IT-a i IT servisa ZU Apoteka Vranje.</p> <p>Svestan sam da nepridržavanje ovih pravila predstavlja povredu radne obaveze usled koje mi može prestati radni odnos i/ili od strane ZU Apoteka Vranje biti pokrenut drugi odgovarajući postupak.</p> <p>Takođe, ovom Izjavom prihvatom da po predočenju od strane ZU Apoteka Vranje izmena i dopuna ovog Pravilnika, iste odmah primenjujem.</p> <p>Datum:</p>										
<table border="1"> <tr> <td><i>Ime i prezime</i></td> <td><i>JMBG</i></td> <td><i>Korisnički nalog</i></td> <td><i>Potpis</i></td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </table>	<i>Ime i prezime</i>	<i>JMBG</i>	<i>Korisnički nalog</i>	<i>Potpis</i>							
<i>Ime i prezime</i>	<i>JMBG</i>	<i>Korisnički nalog</i>	<i>Potpis</i>								

Slika 3. Primer izjave o razumevanju i prihvatanju uslova iz “Pravilnika o primeni informacionih tehnologija”

LITERATURA

- [1] TASIĆ, I. (2014): *Predlog modela zaštite poslovno informacionog sistema apotekarskih ustanova – studija slučaja Apoteka Vranje*, doktorska disertacija, Univerzitet Singidunum, Departman za poslediplomske studije i međunarodnu saradnju, Beograd
- [2] http://os2.zemris.fer.hr/ISMS/politika/2006_kovacevic/Sigurnosna%20Politika.htm