UDC: 006.3/8:004.6.056 Info M str. 4-8

PRIMENA KLJUČNIH INDIKATORA PERFORMANSI U UPRAVLJANJU BEZBEDNOŠĆU PODATAKA
APPLICATION OF KEY PERFORMANCE INDICATORS IN DATA SECURITY MANAGEMENT

Jelena Samardžija, Danica Lečić-Cvetković, Teodora Rajković

REZIME: Primena ključnih indikatora performansi (KPI) definisanih za merenje nivoa bezbednosti podataka na Internetu na konkretnom primeru preduzeća koje se bavi pružanjem usluga merenja nivoa bezbednosti podataka na Internetu je prikazana u ovom radu. Ključne delatnosti koje se posmatraju iz ovog domena se odnose na pružanje usluga odgovora na incidente, operativne sajber-bezbednosti i konsultantske usluge. Na osnovu izmerenih vrednosti definisanih KPI, preduzeća mogu u svakom trenutku da ocene nivo bezbednosti podataka u svom sistemu, ali i da definišu unapređenja i poboljšanja uslova za postizanje visokog niva bezbednosti podataka. Definisani KPI su primenjeni nad podacima odabranog preduzeća i dobijeni su rezultati koji se razlikuju od željenih vrednosti posmatranih KPI. Na osnovu toga se može zaključiti da posmatrano preduzeće treba da poboljša kvalitet usluga koje pruža. Neki od načina jesu angažovanje dodatnih kadrova za rešavanje tekućih problema, kao i uvođenje dodatnih aplikacija ili softvera, koji bi ubrzali proces otklanjanja novonastalih problema.
KLJUČNE REČI: KPI, merenje, Internet, bezbednost podataka, poboljšanje.
ABSTRACT: The application of key performance indicators (KPIs) defined for measuring the level of data security on the Internet is presented in this paper. These KPIs are applied to the company that provides services for measuring the level of data security on the Internet. The main activities observed in this domain relate to the provision of incident response services, operational cyber security, and consulting services. Based on the measured values of the defined KPIs, companies can access the level of data security in their system, but also define improvements for achieving a high level of data security. The defined KPIs were applied to the data of the selected company and obtained results that differ from the desired values of the observed KPIs. Based on that, it can be concluded that the observed company should improve the quality of services it provides. Some of the options are to engage additional staff to solve current problems, as well as the introduction of additional applications or software that would speed up the process of troubleshooting.
KEY WORDS: KPIs, measurement, Internet, data security, improvement.

1. UVOD

Bezbednost podataka je u centru interesovanja savremenog društva zbog naglog porasta broja korisnika Interneta. Podaci koji se čuvaju na računaru, primaju i šalju putem Interneta, mogu da budu izuzetno poverljivi. Na primer, to mogu da budu lični podaci, poput: adrese stanovanja, brojeva platnih kartica, lozinke, kao i podaci koji su namenjeni samo za uži krug korisnika. Da bi se adekvatno upravljalo tehnološkim performansama poslovanja na Internetu, potrebno je da se definišu, analiziraju i prate odgovarajući indikatori performansi.

Primena savremenih informaciono-komunikacionih tehnologija u savremenim uslovima poslovanja predstavlja ključnu snagu konkurentnosti svakog preduzeća, privrede i društva. Već dugi niz godina razvijaju se tehnike i metode za merenje učinka, obima i stepena tehnoloških promena, kao i za analiziranje i praćenje unapređenja rezultata poslovanja nastalih njihovim primenama. Praktično iskustvo i analiza rezultata primene mogu da prošire mogućnosti njihove dalje primene, kroz planiranje, usmeravanje, koordinaciju i kontrolu uvođenja novih tehnologija na svim nivoima jednog preduzeća. Potrebe za primenom indikatora performansi kojima se meri tehnološki i naučni razvoj je od izuzetnog značaja poslednjih nekoliko godina. To je naročito primetno kroz evoluciju novog oblika ekonomije koji rezultuje procesom globalizacije, primenom informaciono-komunikacionih tehnologija. Razvoj nauke i tehnologije nije samo ključni indikator konkurentnosti i ekonomskog rasta jedne zemlje, nego je i od velikog značaja za poboljšavanje kvaliteta života, okruženja i socijalnog razvoja [1]. Ulaganja u razvoj tehnologije i nauke utiču i na razvoj te zemlje, u globalnom smislu. Pojam performansa podrazumeva karakteristike ili pokazatelje rezultata poslovanja preduzeća [2].

Ključne indikatore performansi svako preduzeće određuje individualno. Oni moraju da budu u skladu sa veličinom i strukturom preduzeća, kao i njegovim aktivnostima, procesima i proizvodima. Takođe, *KPI* moraju biti usaglašeni sa ciljevima preduzeća. Od velikog je značaja da se ne zanemari činjenica da upravo primena *KPI* omogućava bolje rezultate poslovanja, ukoliko se posmatraju i prate duži vremenski period. Prema tome, primena *KPI* omogućava povećanje pouzdanosti i unapređenje fleksibilnosti u savremenom poslovanju, što može pozitivno da utiče na povećanje rezultata poslovanja. *KPI* mogu da se definišu za različite hijerarhijske nivoe u preduzeću. Osim na nivou celokupnog preduzeća, mogu da se odrede i na nivou odeljenja, kao i radnih mesta gde se može meriti uspešnost poslovanja nekog zaposlenog [3].

U radu je prikazana primena definisanih *KPI* za merenje nivoa bezbednosti podataka na Internetu na konkretnom primeru preduzeća *Unicom-Telecom* iz Beograda koje se bavi pružanjem usluga merenja nivoa bezbednosti podataka na Internetu. Ovaj rad se sastoji od šest poglavlja. Prvo poglavlje predstavlja uvod u rad. U drugom poglavlju je objašnjen pojam bezbednosti podataka na Internetu. U trećem poglavlju su predstavljeni i objašnjeni termini performansa, indikatori performansi i ključni indikatori performansi, kao i neki od *KPI* koji se koriste u praćenju bezbednosti podataka na Internetu. U četvrtom poglavlju su predstavljeni definisani *KPI* za merenje nivoa bezbednosti podataka na Internetu. U petom poglavlju je prikazana primena definisanih *KPI* za merenje nivoa bezbednosti podataka na Internetu u odabranom preduzeću. U šestom poglavlju su prikazani izvedeni zaključci ovog rada i predstavljeni budući pravci istraživanja.

2. BEZBEDNOST PODATAKA NA INTERNETU

U savremenom društvu koje je globalno povezano, komunikacija između ljudi iz različitih krajeva sveta se obavlja

jeftino i brzo, putem Interneta. Do radikalnih promena u životima ljudi je došlo upravo zbog sve veće upotrebe računara, lakog pristupa Internetu, odnosno primene savremenih informaciono-komunikacionih tehnologija. Danas postoje besplatni *Online* servisi koji korisnicima nude razne mogućnosti za komunikaciju [4]. Da bi se zaštitili poverljivi podaci od neovlašćenog pristupa, neophodno je ograničiti broj ljudi kojima će taj pristup biti dozvoljen, kao i način na koji se njima može pristupiti. To podrazumeva da je pri planiranju sadržaja aplikacija neophodno razmišljati o zaštiti podataka. Potrebno je da se pažljivo konfigurišu softver i server, pažljivo programira, detaljno testira, da se uklanjaju nepotrebni servisi sa *Web* servera i proverava identitet korisnika. Bezbednost kao pojam pripada grupi višeznačnih apstraktnih reči koja predstavlja zaštićenost pojedinog subjekta od raznih vrsta ugrožavanja. U modernoj literaturi se najčešće piše o sveobuhvatnoj bezbednosti koja obuhvata: političku, vojnu, ekonomsku, informacionu, energetsku bezbednost i slično. Ta sveobuhvatna bezbednost podrazumeva veliki broj komponenti koje se prepliću.

Glavni element nacionalne bezbednosti je informaciona bezbednost (*INFOSEC - Information Security*), koja obuhvata zaštićenost interesa države, ličnosti i društva od raznih pretnji i rizika u okviru informacione sfere [5]. Kada se posmatra informaciona bezbednost, akcenat se stavlja na integritet, raspoloživost i tajnost informacija. Zaštita integriteta podataka podrazumeva obezbeđivanje celovitosti i tačnosti poruke koja se šalje, tj. sprečava se mogućnost promene poruke bez obzira da li se radi o nenamernom ili namernom oštećenju. Raspoloživost resursa podrazumeva servise koji pružaju mogućnost obezbeđivanja ovlašćenim korisnicima pristup informacijama kad god su im potrebne. Tajnost podataka podrazumeva dostupnost informacija samo ovlašćenim licima [6]. Kada je u pitanju bezbednost informacija, veoma je bitno da se zadovolje sledeća svojstva informacija [7]: poverljivost ili privatnost (*Privacy*), raspoloživost (*Availability*) i integritet (*Integrity*), dok se često dodaju neopozivost (*Non-Repudiation*) i autentičnost (*Authentication*).

Glavni cilj privatnosti je da se dozvoli pristup informacijama samo autorizovanim licima, programima i procesima. Poverljivost informacija se odnosi na nacionalnu, industrijsku ili ličnu poverljivost. Integritet nastoji da obezbedi informacije i resurse (softver i hardver) koji mogu da budu uništeni ili modifikovani uz definisanu i posebnu autorizaciju. Glavni cilj raspoloživosti se odnosi na usluge i informacije koje moraju da budu dostupne u bilo kom trenutku adekvatnim korisnicima. Odnosno, sistem koji se bavi pružanjem takvih usluga mora da funkcioniše u ograničenom i određenom vremenu i to samo kada se od njega to i zahteva. Kada se posmatra sa operativnog nivoa, raspoloživost informacija podrazumeva prikladan nivo usluge i prihvatljivo vreme odgovora sistema. Međutim, sa nivoa bezbednosti informacija, raspoloživost je sposobnost zaštite od mogućnosti ponovnog započinjanja rada sistema ili zaštite od štetnih događaja. Kod savremenih informacionih sistema, raspoloživost je neophodna, kako za bezbednost ljudskih života, tako i za normalno izvršavanje aktivnosti. Autentičnost predstavlja karakteristiku bezbednosti koja nastoji da se odredi validnost i vrednost prenosa, pošiljaoca ili poruke. Osim toga, uz pomoć autentičnosti može da se kontroliše i autorizacija korisnika, kako bi svaki korisnik primio informacije koje su specifične i njemu potrebne. Neopozivost ima za cilj obezbeđenje toka komunikacije. Uz pomoć neopozivosti može da se postigne da pošiljaoci imaju dokaz da su poslali informaciju, ali i to da primalac poseduje podatak o identifikaciji pošiljaoca. Na taj način se postiže da na kraju nijedan od učesnika ne može da negira transakciju koja se izvršila [7]. Međutim, iako ne postoji opšta definicija „digitalne bezbednosti“, može se zaključiti da su pojmovi „informaciono obezbeđenje“ i „informaciona bezbednost“ uključeni u široki koncept digitalne bezbednosti.

Pojam „digitalne bezbednosti“ danas se koristi da označi skup aktivnosti i tehnika koje su osmišljene kako bi se zaštitilo od napada na informacije, usluge i mreže računara [8]. Glavni cilj koji treba da se definiše ovim pojmom se odnosi na osmišljavanje i poboljšavanje postojećih aktivnosti kako bi se nivo zaštite povećao uz smanjivanje pretnji. Koncept digitalne bezbednosti podrazumeva da se holistički pristupa istraživanju uz suprotstavljanje mogućim pretnjama informacionih sistema sa stanovišta matematičkih i informatičkih nauka [5].

3. PERFORMANSE, INDIKATORI PERFORMANSI I KLJUČNI INDIKATORI PERFORMANSI

Sposobnost preduzeća da upravlja svojim performansama, odnosno da definiše, meri, analizira i poboljša svoje performanse je od izuzetnog značaja za njen budući razvoj [9]. Prema autoru *Neely* [10] pojam „performansa“ se definiše kao: karakteristika ili pokazatelj rezultata funkcionisanja preduzeća. Merenje performansi predstavlja kontinuirano praćenje i izveštavanje o dostignućima posmatranog procesa. Rezultat merenja performansi je indikator performansi. U cilju potpune identifikacije performansi, potrebno je identifikovati indikatore performansi, načine merenja, referentne vrednosti za poređenje rezultata, kao i izvor i pouzdanost podataka koji se koriste [11].

Indikatori performansi su alati za razumevanje, upravljanje i poboljšanje aktivnosti preduzeća na osnovu kojih je moguće sagledati koliko se dobro odvijaju procesi, da li se ispunjavaju postavljeni ciljevi, da li su kupci zadovoljni, da li su svi procesi pod kontrolom, i ukazuju na mesta gde su neophodna poboljšanja procesa [12]. Većina indikatora performansi se odnosi se na sledeće aspekte procesa [13]: efektivnost (karakteristika procesa koja ukazuje na stepen do kojeg je rezultat procesa usklađen sa zahtevima), efikasnost (karakteristika procesa koja ukazuje na stepen do kojeg proces proizvodi tražene rezultate uz minimalne troškove resursa) i briga o korisnicima (stepen zadovoljstva korisnika procesa). Indikatori performansi predstavljaju kvantitativne i kvalitativne pokazatelje, uz pomoć kojih se na direktan ili indirektan način može vršiti procena ili merenje nivoa ili stepena ostvarenja nekih ciljeva, kao i procena brzine, vremena ili roka ostvarivanja ciljeva. Takođe, indikatori performansi mogu da se definišu kao kvantitativni ili numerički indikatori ostvarivanja određenog cilja [14].

Definisanje jedne performanse obuhvata [1]:

- Identifikovanje procesa/celine/objekata na koje se odnosi performansa;
- Određivanje operacionog značenja performanse;

- Kontekst ispoljavanja konkretne performanse;
- Načine uticanja na performansu;
- Načine merenja i identifikovanja performanse;
- Konkretne učinke koji proizilaze iz performanse koja se definiše.

Indikatori performansi koji su od najvećeg značaja za preduzeće se nazivaju ključni indikatori performansi (*Key Performance Indicators – KPIs*). *KPI* su oni indikatori performansi koji se fokusiraju na performanse preduzeća koje su najkritičnije za sadašnji i budući uspeh preduzeća [3]. Oni predstavljaju skup indikatora performansi koje je unapred izabrao ili definisao menadžment koji snažno odražava kritične faktore koji su od posebnog interesa za performanse posmatranog preduzeća [9]. Preduzeća primenjuju *KPI* na više nivoa kako bi procenile svoj uspeh u postizanju ciljeva. *KPI* na visokom nivou se fokusiraju na ukupne performanse preduzeća, dok se *KPI* na niskom nivou fokusiraju na procese u odeljenjima [15].

4. *KPI* ZA MERENJE NIVOA BEZBEDNOSTI PODATAKA NA INTERNETU

Za praćenje bezbednosti podataka na Internetu koriste se *KPI*. Autori *Onwubiko* i *Ouazzane* [16] navode da se *KPI* koriste za praćenje tekućih bezbedonosnih incidenata i narušavanja bezbednosti, kao i za kreiranje poslovnih izveštaja i merenja povraćaja ulaganja u bezbednost (eng. *Return on Security Investment - RoSI*). Autori *Onwubiko* i *Onwubiko* [17] navode da se za kreiranje tih poslovnih izveštaja prati broj detektovanih sajber incidenata, kao i broj sprečenih sajber ili terorističkih napada. Autori *Kure, Islam* i *Razzaque* [18] smatraju da su *KPI* za praćenje poverljivosti (koji omogućavaju otkrivanje osetljivih podataka protiv neovlašćenih, internih i eksternih korisnika i zlonamernih napadača) i *KPI* za merenje autentičnosti (koji poboljšavaju tehnologiju identifikacije i verifikacije ovlašćenog korisnika kako bi pružili sigurnost, jednostavnost korišćenja i administraciju, dok ovlašćenog korisnika identifikuju prema njegovim specifičnim informacijama i vrsti usluge) jako bitni za praćenje bezbednosti podataka na Internetu. Autori *Gunes*, *Kayisoglu* i *Bolat* [19] definišu poverljivost, integritet, dostupnost, usluge, bezbednost, fleksibilnost i realnost kao *KPI* za sajber bezbednost. Poverljivost, integritet i dostupnost su tri najvažnija *KPI*. Poverljivost se obezbeđuje zaštitom resursa, podataka i objekata od neovlašćenog pristupa, integritet je obezbeđen zaštitom podataka od neovlašćenih promena, dok se dostupnost obezbeđuje tako što ovlašćeni korisnici pristupaju sistemima po potrebi.

U ovom poglavlju je predstavljeno pet *KPI* definisanih na osnovu uočenih problema koji su se ponavljali u posmatranom preduzeću, a koji se koriste za merenje nivoa bezbednosti podataka na Internetu. Cilj njhove primene je da se unaprede rezultati poslovanja posmatranog preduzeća, odnosno unapredi pružanje usluga merenja nivoa bezbednosti podataka na Internetu.

1. Ukupan procenat rešenih bezbednosnih incidenata – *KPI BI*.

Ovaj indikator predstavlja osnovni ključni indikator performansi za merenje bezbednosti podataka, koji se računa kao odnos ukupnog broja rešenih bezbednosnih incidenata i ukupnog broja bezbednosnih incidenata. Formula za izračunavanje *KPI BI* prikazana je izrazom (1).

$$BI = \frac{BI_{ur}}{BI_u} \cdot 100\ [\%] \tag{1}$$

Gde su:

- *BI* – Ukupan procenat rešenih bezbednosnih incidenata [%];
- BI_{ur} – Ukupan broj rešenih bezbednosnih incidenata [1];
- BI_u – Ukupan broj bezbednosnih incidenata [1].

Željena vrednost *KPI BI* je ≈ 50[%].

2. Srednje vreme prepoznavanja bezbednosnih incidenta – *KPI SVP.*

Vrednost ovog *KPI* pokazuje koliko je vremena potrebno da se prepozna napad na podatke. Izračunava se kao zbir srednjeg vremena od pojave bezbednosnih incidenata i srednjeg vremena otkrivanja incidenata. Da bi se izračunao ovaj indikator performansi potrebno je da se sabere vreme od početka prekida rada sistema, neispravnosti usluge ili drugih bezbednosnih problema i vreme potrebno za otkrivanje problema koji se pojavio. Formula za izračunavanje *KPI SVP* prikazana je izrazom (2).

$$SVP = SV_{pbi} + SV_{ibi}[\text{min}] \tag{2}$$

Gde su:

- *SVP* – Srednje vreme prepoznavanja bezbednosnih incidenata [min];
- SV_{pbi} – Srednje vreme od pojave bezbednosnih incidenata [min];
- SV_{ibi} – Srednje vreme identifikovanja bezbednosnih incidenata [min].

Željena vrednost indikatora *KPI SVP* je ≈ 20 [min].

3. Srednje vreme otklanjanja problema – *KPI SVO.*

Vrednost ovog *KPI* pokazuje količinu vremena koja je potrebna za otklanjanje problema nakon što je utvrđen napad na podatke. Ovaj *KPI* se izračunava kao zbir srednjeg vremena zadržavanja prilikom utvrđivanja napada i srednjeg vremena rešavanja problema. To je zapravo vreme između utvrđivanja postojanja bezbednosnih problema i trenutka kada se izvrši oporavak sistema nakon napada. Formula za izračunavanje *KPI SVO* prikazana je izrazom (3).

$$SVO = SV_z + SV_r[\text{min}] \tag{3}$$

Gde su:

- *SVO* – Srednje vreme otklanjanja problema nakon što je utvrđen napad [min];
- SV_z – Srednje vreme zadržavanja prilikom utvrđivanja napada [min];
- SV_r – Srednje vreme rešavanja problema prilikom utvrđivanog napada [min].

Željena vrednost indikatora *KPI SVO* je ≈ 20 [min].

4. Procenat neprekidnog rada softvera za bezbednost podataka – *KPI PNRS.*

Vrednost ovog *KPI* pokazuje koliko često neki softver koji se koristi za održavanje bezbednosti podataka radi u toku jednog meseca. Izračunava se kao razlika broja dana u posmatranom mesecu i vremena zastoja (u danima) usled ažuriranja ovog softvera ili usled napada na podatke u posmatranom mesecu, podeljeno sa brojem dana u posmatranom mesecu. Vremenska jedinica u kojoj se vrednost ovog *KPI* izražava u ovom radu je prikazan u danima, ali može da bude i u drugim vremenskim jednicama. Formula za izračunavanje *KPI PNRS* prikazana je izrazom (4).

$$PNRS = \frac{BD - VZ}{BD} \cdot 100\ [\%] \tag{4}$$

Gde su:

- *PNRS* – Procenat neprekidnog rada softvera za bezbednost podataka na mesečnom nivou [%];
- *BD* – Broj dana u mesecu [dan];
- *VZ* – Vreme zastoja usled ažuriranja softvera za bezbednost podataka ili usled napada na podatke [dan].

Željena vrednost indikatora *KPI PNRS* je 100 [%].

5. Ukupan broj grešaka ili problema na dnevnom nivou u posmatranom mesecu – *KPI UBG.*

Problemi ili greške u radu programa za održavanje bezbednosti podataka se javljaju svakodnevno, a oni koji su najviše kritični se moraju pratiti tokom dužeg vremenskog perioda i detaljno analizirati. Izračunava se kao zbir broja prijavljenih grešaka od strane zaposlenih na dnevnom nivou (interno) i broja grešaka koje prijavljuju korisnici na dnevnom nivou (eksterno) u odnosu na broj dana u posmatranom mesecu prilikom korišćenja određenog softvera. Indikator *KPI UBG* se računa za prethodni mesec, kako bi se izračunao broja grešaka ili problema koji su se javljali u prethodnom mesecu koji se posmatra, sa ciljem da se donesu odluke za poboljšanje, ukoliko je to neophodno. Visoka vrednost ovog *KPI* ukazuje na to da postoje problemi u funkcionisanju posmatranog softvera, koji se moraju identifikovati i otkloniti. Zbog toga je od velikog značaja pratiti ovaj *KPI.* Formula za izračunavanje *KPI UBG* prikazana je izrazom (5).

$$UBG = \frac{BG_i + BG_e}{BD}\ [1/dan] \tag{5}$$

Gde su:

- *UBG* – Ukupan broj grešaka ili problema na dnevnom nivou u posmatranom mesecu [1/*dan*];
- BG_i – Broj grešaka prijavljenih interno od strane zaposlenih na dnevnom nivou u posmatranom mesecu [1];
- BG_e – Broj grešaka prijavljenih eksterno od strane korisnika na dnevnom nivou u posmatranom mesecu [1];
- *BD* – Broj dana u posmatranom mesecu [dan].

Željena vrednost indikatora *KPI UBG* je da bude što manja, odnosno ≈ [0/*dan*].

5. PRIMER PRIMENE *KPI* ZA MERENJE NIVOA BEZBEDNOSTI PODATAKA NA INTERNETU

U nastavku rada prikazana je primena prethodno definisanih *KPI* za merenje nivoa bezbednosti podataka na Internetu na konkretnom primeru preduzeća *Unicom-Telecom* iz Beograda. Preduzeće *Unicom* se bavi pružanjem usluga merenja nivoa bezbednosti podataka na Internetu. Sastoji se iz dva povezana preduzeća. Prvo preduzeće je *Unicom-Telecom* koje je sistem integrator, što znači da se bavi isporukom *IT* poslovnih rešenja preduzećima u Republici Srbiji i u regionu. Drugo preduzeće je *Unicom-Systems* koje je servis provajder za usluge sajber-bezbednosti, u okviru koje postoji organizaciona jedinica *CERT/SOC (Security Operations Center*). *UniCERT* je organizaciona jedinica unutar preduzeća *Unicom-Systems* koja za cilj ima da pruži usluge iz domena sajber bezbednosti. Delatnosti koje su ključne iz ovog domena se odnose na pružanje usluga odgovora na incidente, operativne sajber-bezbednosti i konsultantske usluge. Vrednosti pomoću kojih se u ovom radu izračunavaju posmatrani *KPI* su preuzeti iz internih izvora ovog preduzeća. Primena prethodno definisanih *KPI* za merenje nivoa bezbednosti podatka na Internetu je predstavljena u Tabeli 1.

Tabela 1: Primena *KPI* za merenje nivoa bezbednosti podatka na Internetu na osnovu podataka preduzeća *Unicom-Telecom*

Naziv *KPI*	Vrednost *KPI*	Komentar
1. Ukupan procenat rešenih bezbednosnih incidenata – *KPI BI*	$BI = \frac{25}{55} \cdot 100[\%] \approx 45[\%]$	Vrednost *KPI BI* je manja od željene vrednosti za 5 [%]
2. Srednje vreme prepoznavanja bezbednosnih incidenta – *KPI SVP*	$SVP = 8 + 10 = 18$ [min]	Vrednost *KPI SVP* je manja od željene vrednosti za 2 [min]
3. Srednje vreme otklanjanja problema – *KPI SVO*	$SVO = 7 + 15 = 22$ [min]	Vrednost *KPI SVO* je veća od željene vrednosti za 2 [min]
4. Procenat neprekidnog rada softvera za bezbednost podataka– *KPI PNRS*	$PNRS = \frac{30-2}{30} \cdot 100[\%] \approx 93[\%]$	Vrednost *KPI PNRS* je manja od željene vrednosti za 7 [%]
5. Ukupan broj grešaka ili problema na dnevnom nivou u posmatranom mesecu – *KPI UB*G	$UBG = \frac{3+1}{30} \approx 0[1/dan]$	Vrednost *KPI UBG* je jednaka željenoj vrednosti

Na osnovu prikazanih rezultata primene definisanih *KPI* za merenje nivoa bezbednosti podataka na Internetu, može da se zaključi da je posmatrano preduzeće identifikovalo većinu rizika koji su vezani za bezbednost podataka koje koriste u poslovanju, ali da i dalje ima mesta za unapređenje. S obzirom da dobijeni rezultati ukazuju na odstupanja od željenih vrednosti posmatranih *KPI*, posmatrano preduzeće treba da sprovede odgovarajuće mere za unapređenje usluga koje pruža. Te mere treba da budu u skladu sa mogućnostima i dostupnim resursima preduzeća, a neke od njih su predstavljene u nastavku. Kada je u pitanju ukupan procenat rešenih bezbednosnih incidenata – *KPI BI*, mere koje posmatrano preduzeće treba da preduzme se odnose na unapređenje broja rešenih bezbednosnih incidenata, što se može postići povećanjem broja angažovanih kadrova koji se bave rešavanjem ovakvih problema. Takođe, postoji prostor za unapređenje vrednosti indikatora Srednje vreme prepoznavanja bezbednosnih incidenata – *KPI SVP,* kroz uvođenje dodatnih aplikacija ili softvera koji će skratiti vreme prepoznavanja bezbednosnih incidenata koji su se desili. Vrednost indikatora Srednje vreme otklanjanja problema – *KPI SVO* može da se poboljša

kroz angažovanje dodatnih kadrova koji će raditi na otklanjanju problema ili kroz korišćenje usluga drugih preduzeća koja se bave tim poslom. Kada je u pitanju vrednost indikatora Procenat neprekidnog rada softvera za bezbednost podataka – *KPI PNRS*, predlog je da se uvede i drugi softver koji će da bude redundantan sa postojećim softverom, kako bi se vrednost ovog indikatora povećala. U tom slučaju, ukoliko dođe do prekida rada jednog softvera, sve aktivnosti se automatski prenose na drugi softver, koji nastavlja sa radom. Vrednost indikatora Ukupan broj grešaka ili problema na dnevnom nivou u posmatranom mesecu – *KPI UBG* je na nivou željene vrednosti i ne zahteva dodatna poboljšanja.

6. ZAKLJUČAK

U savremenim uslovima poslovanja, uzevši u obzir veoma brz razvoj informaciono-komunikacionih tehnologija, bezbednost podataka na Internetu je veliki izazov, te se može zaključiti da ne postoji mogućnost potpune zaštite podataka, ali da postoji mogućnost da se količina privatnih podataka dostupnih na Internetu svede na minimum i da se oni zaštite. Takođe, moguće je koristiti programe za zaštitu podataka, odnosno za identifikaciju napada na bezbednost podataka, kao i za oporavak sistema nakon napada. Potrebno je konstantno meriti bezbednost podataka u jednom preduzeću, što je moguće primenom *KPI,* koji su predstavljeni u ovom radu. Na osnovu izmerenih vrednosti, ta preduzeća mogu u svakom trenutku da ocene nivo bezbednosti podataka u svom sistemu, ali i da uvedu unapređenja i poboljšanja uslova za visok nivo bezbednosti podataka. Kao potreba javlja se optimizacija bezbednosti podataka, sa fokusom na povećanje efikasnosti kroz ulaganje u nove i inovativne tehnologije za poboljšanje zaštite podataka. Međutim, najveća prepreka pri podizanju svesti preduzeća i korisnika o važnosti bezbednosti podataka na Internetu jeste upravo nerazumevanje pretnji kojima su izloženi, kao i nedovoljna informisanost o visokotehnološkom kriminalu. Zaključak jeste da mnogi napadi i krađe podataka i identiteta mogu biti sprečeni ukoliko se svi korisnici ponašaju odgovorno i pažljivo biraju koje podatke i na koji način razmenjuju putem Interneta.

Jedan od pravaca budućeg istraživanja autora ovog rada jeste da se sprovedu dodatna istraživanja na temu unapređenje merenja nivoa bezbednosti podataka na Internetu, kako bi se definisalo još *KPI* koji se odnose na praćenje bezbednosti podataka na Internetu, a koji su od velikog značaja za preduzeća. Drugi pravac budućeg istraživanja autora ovog rada je da se definisani *KPI* primene u još nekoliko preduzeća, koja se bave pružanjem usluga merenja nivoa bezbednosti podataka na Internetu. Na osnovu toga je moguće uraditi uporednu analizu, kako bi se doneli dodatni zaključci u vezi poboljšanja zaštite bezbednosti podataka koji se razmenjuju na Internetu.

LITERATURA

[1] Marr, B. (2012). *Key Performance Indicators (KPI): The 75 measures every manager needs to know*. Pearson UK.

[2] Kerzner, H. (2017). *Project Management Metrics, KPIs, and Dashboards: A Guide to Measuring and Monitoring Project Performance*. John Wiley & Sons.

[3] Parmenter, D. (2015). *Key Performance Indicators: Developing, Implementing, and Using Winning KPIs*. John Wiley & Sons.

[4] Mikarić, B. N., Blagojević, M. M., & Trajković, D. (2016). Privatnost na Internetu - Mit ili realnost. *Trendovi u poslovanju*, *2*(8), 67-72.

[5] Sinkovski, S. (2005). Informaciona bezbednost - komponenta nacionalne bezbednosti. *Vojno delo, 57,* 31-81.

[6] Denning, D. (2001). Cyberwarriors, Activists and Terrorists Turn to Cyberspace. *Harvard International Review, 23*(2), 70-75.

[7] Vuletić, D. (2017). Sajber bezbednost. *Integralna bezbednost Republike Srbije*, 169-184.

[8] Putnik, N. (2009). *Sajber prostor i bezbednosni izazovi*. Beograd: Fakultet bezbednosti.

[9] Samsonowa, T. (2011). *Industrial Research Performance Management: Key Performance Indicators in the ICT Industry*. Springer Science & Business Media.

[10] Neely, A. (2002). *Business Performance Measurement – Theory and Practice*. Cambridge University Press.

[11] Atanasov, N. (2016). *Model za izbor adekvatnog skupa indikatora performansi u upravljanju proizvodnjom* (doktorska disertacija). Beograd: Fakultet organizacionih nauka.

[12] Eccles, R. G. (1991). The Performance Measurement Manifesto. *Harvard business review*, *69*(1), 131-137.

[13] Franceschini, F., Galetto, M., & Maisano, D. (2018). *Designing Performance Measurement Systems: Theory and Practice of Key Performance Indicators*. Springer.

[14] Fabig, C., Haasper, A. (2018). *Secure Your Business: Insights to Governance, Risk, Compliance & Information Security*, 2nd edition. Books on Demand.

[15] Pîrlog, R., & Balint, A. O. (2016). An analyze upon the influence of the Key Performance Indicators (KPI) on the decision process within Small and Medium-sized Enterprises (SME). *Hyperion International Journal of Econophysics & New Economy*, *9*(1), 173-185.

[16] Onwubiko, C., & Ouazzane, K. (2022). Challenges Towards Building an Effective Cyber Security Operations Centre. *arXiv preprint arXiv:2202.03691*. DOI: 10.48550/arXiv.2202.03691

[17] Onwubiko, C., & Onwubiko, A. (2019). Cyber KPI for Return on Security Investment. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA),* 1-8. DOI: 10.1109/CyberSA.2019.8899375

[18] Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences, 8*(6), 898. DOI: 10.3390/app8060898

[19] Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber Security Risk Assessment for Seaports: A Case Study of a Container Port. *Computers & Security*, *103*, 102196. DOI: 10.1016/j.cose.2021.102196

Jelena Samardžija, Univerzitet u Beogradu, Fakultet organizacionih nauka
Kontakt: jelenasamardzija25@gmail.com
Oblast interesovanja: Informacione tehnologije, Bezbednost informacionih sistema, Digitalna bezbednost, Bezbednost mreže.

Prof. dr Danica Lečić-Cvetković, redovni profesor, Univerzitet u Beogradu, Fakultet organizacionih nauka
Kontakt: danica.lecic-cvetkovic@fon.bg.ac.rs
Oblast interesovanja: Operacioni menadžment, Upravljanje proizvodnjom i pružanjem usluga, Indikatori performansi u upravljanju proizvodnjom i pružanjem usluga, Elektronsko upravljanje proizvodnjom i pružanjem usluga

Teodora Rajković, MSc, Univerzitet u Beogradu, Fakultet organizacionih nauka
Kontakt: teodora.rajkovic@fon.bg.ac.rs
Oblast interesovanja: Operacioni menadžment, Upravljanje proizvodnjom i pružanjem usluga, Indikatori performansi u upravljanju proizvodnjom i pružanjem usluga, Elektronsko upravljanje proizvodnjom i pružanjem usluga