



UNIVERZITET SINGIDUNUM
FAKULTET ZA INFORMATIKU I MENADŽMENT
Beograd, Danijelova 32

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE
MASTER STUDIJE

Časlav Maksić

POBOLJŠAVANJE PROCESA ZAŠTITE INFORMACIJA

– Master Rad –

Mentor:

Doc. dr Gojko Grubor

Kandidat:

Časlav Maksić

Beograd, jun 2011

Sažetak

Ovaj rad se bavi metrikom zaštite informacija, kao kvantitativnom metodom analize merenja performansi aktivnosti zaštite. Metrike zaštite informacija uglavnom su predmet istraživanja specijalizovanih grupa za zaštitu informacija i menadžera sistema zaštite informacija. Rezultati tih istraživanja najčešće ukazuju na probleme izrade programa metrike zaštite, izbora odgovarajuće metrike i načina prezentovanja rezultata. U cilju razumevanja ovih problema, u radu su korišćeni najrelevantniji izvori koji se isključivo odnose na probleme primene metrika zaštite informacija u poslovnim organizacijama. Definisana je metodologija istraživanja, pojam metrike zaštite informacija, opisan je metod za izradu programa zaštite informacija i predstavljeni su praktični primeri i saveti za primenu programa metrike zaštite. Kroz rad će se pokazati kako metrika zaštite informacija može pomoći menadžerima zaštite i poslovodstvu u efektivnom upravljanju poslovnim procesima.

U ovom radu date su osnovne informacije o tome, šta je i kako se vrši merenje performansi zaštite informacija. Pored toga, ovde su definisani različiti tipovi merenja, kao i ključni aspekti za izradu uspešnog programa merenja zaštite informacija i navedene su prednosti korišćenja merenja zaštite za upravljanje resursima i donošenje poslovnih odluka.

Ovaj rad se, pre svega, oslanja na međunarodne standarde i naučna istraživanja svetski priznatih univerziteta u oblasti zaštite informacija, koji su uspostavili zvanične preporuke najboljih praksi zaštite informacija, razvili i publikovali besplatne softverske alate za podršku u praktičnoj implementaciji standardnih preporuka zaštite, a jedan od tih alata ovde je iskorišćen za uspostavljanje procesa merenja uticaja bezbednosnih incidenata na poslovanje.

Rad može koristiti rukovodiocima sistema zaštite informacija za izradu programa merenja performansi zaštite informacija, koji će, pored poboljšanja procesa zaštite, koristiti zainteresovanim stranama za donošenje odluka i ostvarenje bezbednosnih zahteva klijenata. Uspostavljanjem veze između informacionog sistema, procesa zaštite i poslovnih ciljeva, otvara se prostor za demonstraciju značaja zaštite informacija u poslovanju.

Ključne reči: Metrika zaštite informacija, program merenja zaštite informacija, merenje performansi zaštite informacija, kontrole zaštite, zrelost procesa, kapacitet procesa.

Abstract

This paper deals with information security metrics, as a quantitative method for analysis of security performance measurements. Information security metrics are mostly subjects of researches conducted by specialized groups in charge of information security and information systems security managers. Results of such researches mostly point out the problems in development of security metrics programs, choice of suitable metrics and ways of their presentation. Trying to overcome the mentioned problems, this paper relies on the most relevant sources, related exclusively to the problems of application of information security metrics in business organizations.

The definition of research methodology and notion of information security metrics is also part of this paper, and also, methods for development of information security metrics program are described and several practical examples and advices for security metrics application are displayed. This paper will demonstrate how the information security metrics can help the security and business managers to effectively make decisions.

This paper encloses central information on measurements of information security performance and how these measurements are conducted. Besides, the types of measurements are defined, and key aspects for creation of successful measurement program are presented. Also, this paper offers insight in advantages of measurement usage for resource management and adoption of business decisions.

This paper can be useful to information security systems managers in the development of performances of information security which will, in addition to improvement of security process, be valuable to decision-making stakeholders. Establishing the connection between information system, security process and organization goals, allows the demonstration of significance of information security for organization business.

Keywords: Information security metrics, information security measurement program, information security performance measurement, security controls, process maturity, process capability.

SADRŽAJ

Sažetak	2
Abstract	3
PREGLED SLIKA	vi
PREGLED TABELA	vi
1 METODOLOGIJA ISTRAŽIVAČKOG RADA.....	7
1.1 Uvodne napomene i obrazloženje rada	7
1.2 Predmet istraživanja.....	7
1.3 Osnovna hipoteza.....	8
1.4 Radna hipoteza	8
1.5 Ciljevi istraživanja.....	9
1.6 Metodi istraživanja	9
2 Primena metrike u cilju poboljšavanja procesa zaštite informacija.....	11
2.1 Osnovna podela metrike u zaštite informacija	13
2.1.1 Karakteristike i značaj metrike u zaštiti informacija	13
<i>Dobre metrike zaštite informacija</i>	<i>15</i>
<i>Loše metrike zaštite informacija.....</i>	<i>17</i>
<i>Značaj metrike zaštite informacija za organizaciju.....</i>	<i>17</i>
2.1.2 Glavni razlozi za korišćenje metrike u zaštiti informacija	18
2.2 Tipovi merenja i njihova zavisnost od zrelosti programa zaštite informacija.....	19
2.2.1 Merenje implementacije.....	20
2.2.2 Merenje efektivnosti/efikasnosti.....	20
2.2.3 Merenje uticaja	20
2.3 Uspostavljanje programa merenja zaštite informacija	21
2.3.1 Definisanje strateških i taktičkih ciljeva programa metrike	22
2.3.2 Izbor metrike	23
<i>Definisanje i razumevanje zahteva zainteresovanih strana</i>	<i>24</i>
<i>Identifikovanje ulaza sa rukovodstvom i osobljem</i>	<i>24</i>
<i>Obezbeđenje finansijskih sredstava</i>	<i>25</i>
<i>Najčešće korišćene metrike zaštite informacija</i>	<i>25</i>
2.3.3 Razvoj strategije za primenu metrike	26
<i>Prikupljanje ulaznih podataka za metrike zaštite informacija</i>	<i>26</i>
<i>Prikupljanje kontekstualnih podataka</i>	<i>28</i>
<i>Normalizacija i skladištenje podataka.....</i>	<i>28</i>
2.3.4 Uspostavljanje referentnih performansi i ciljeva poboljšanja	28
2.3.5 Određivanje načina prezentovanja metrike	28
<i>Najčešće forme prezentovanja metrika zaštite informacija</i>	<i>29</i>
<i>Usklađivanje prezentacije prema zainteresovanim stranama.....</i>	<i>30</i>
<i>Izbor načina prezentovanja</i>	<i>31</i>
<i>Instrument tabla.....</i>	<i>31</i>
<i>Komparativna tabela rezultata</i>	<i>32</i>
<i>Mogućnosti za proširenje komparativne tabele rezultata.....</i>	<i>33</i>
2.3.6 Definisanje akcionog plana i akcija za izvođenje programa metrike zaštite.....	33

2.3.7	Uspostavljanje formalnog ciklusa preispitivanja programa metrike	34
	<i>Preispitivanje namene metrike zaštite</i>	34
	<i>Preispitivanje prezentacione forme</i>	34
2.4	Implementacija programa merenja zaštite informacija.....	34
2.4.1	Priprema za prikupljanje podataka	35
2.4.2	Prikupljanje i analiza podataka.....	35
2.4.3	Identifikovanje korektivnih akcija	36
2.4.4	Planiranje primene korektivnih akcija	37
2.4.5	Primena korektivnih akcija.....	37
2.5	Obrasci za primenu merenja performansi zaštite informacija.....	37
2.6	Model merenja performansi zaštite informacija	40
2.6.1	Elementi modela merenja performansi zaštite informacija i primeri merenja	41
	<i>Osnovna mera i metod merenja</i>	42
	<i>Izvedena mera i funkcija merenja.....</i>	42
	<i>Indikatori performansi i analitički model</i>	42
	<i>Rezultati merenja i kriterijumi za donošenje odluka</i>	42
2.6.2	Odgovornost rukovodstva u programu merenja zaštite informacija.....	44
2.7	Primena modela merenja performansi zaštite informacija.....	44
2.7.1	Definisanje područja primene merenja	45
2.7.2	Identifikovanje informacionih potreba	45
2.7.3	Izbor objekata i atributa merenja	46
2.7.4	Izrada konstrukcije merenja	46
	<i>Izbor merenja.....</i>	46
	<i>Određivanje metoda merenja</i>	46
	<i>Definisanje funkcije merenja.....</i>	47
	<i>Izbor analitičkog modela.....</i>	47
	<i>Utvrđivanje indikatora merenja</i>	47
	<i>Definisanje kriterijuma za donošenje odluka.....</i>	47
	<i>Identifikovanje zainteresovanih strana</i>	48
2.8	Evaluacija i unapređenje programa merenja zaštite informacija	48
2.8.1	Identifikovanje kriterijuma evaluacije programa merenja zaštite informacija.....	48
2.8.2	Nadzor, preispitivanje i evaluacija programa merenja zaštite informacija	49
2.8.3	Implementacija unapređenja.....	49
3	STUDIJA SLUČAJA: USPOSTAVLJANJE KAPACITETA ZA MERENJE	
	UTICAJA BEZBEDNOSNIH RIZIKA	50
3.1	Uvod	50
3.2	Uspostavljanje kapaciteta merenja uticaja bezbednosnog rizika	50
3.2.1	Procena uticaja.....	50
	<i>Prioritetizacija kapaciteta sistema</i>	52
	<i>Identifikovanje imovine sistema.....</i>	52
	<i>Izbor metrike uticaja</i>	53
	<i>Identifikovanje odnosa među metrikama</i>	53
	<i>Identifikovati i karakterizacija uticaja.....</i>	53
	<i>Praćenje uticaja.....</i>	54

3.2.2	Procena pretnji.....	54
	<i>Identifikovanje pretnji koje su posledica aktivnosti čoveka.....</i>	<i>55</i>
	<i>Određivanje merne jedinice pretnje</i>	<i>55</i>
	<i>Procena kapaciteta agenta pretnje.....</i>	<i>55</i>
	<i>Procena verovatnoće pojave pretnje</i>	<i>56</i>
	<i>Identifikovanje prirodnih pretnji</i>	<i>56</i>
	<i>Praćenje promena pretnji i njihovih karakteristika.....</i>	<i>56</i>
3.2.3	Procena ranjivosti	57
	<i>Izbor metoda analize ranjivosti.....</i>	<i>58</i>
	<i>Identifikovanje ranjivosti</i>	<i>59</i>
	<i>Prikupljanje podataka o ranjivostima</i>	<i>59</i>
	<i>Agregiracija ranjivosti sistema</i>	<i>60</i>
	<i>Praćenje promena ranjivosti i njihovih karakteristika</i>	<i>60</i>
3.2.4	Procena bezbednosnog rizika	60
	<i>Izbor metoda za analizu rizika</i>	<i>61</i>
	<i>Identifikovanje izloženosti</i>	<i>61</i>
	<i>Procena rizika izloženosti</i>	<i>62</i>
	<i>Procena ukupne neodređenosti</i>	<i>62</i>
	<i>Prioritetizacija rizika.....</i>	<i>63</i>
	<i>Praćenje rizika i njihovih karakteristika.....</i>	<i>63</i>
3.2.5	Izgradnja bezbednosne garancije.....	63
	<i>Identifikovanje ciljeva bezbednosne garancije.....</i>	<i>64</i>
	<i>Definisanje strategije bezbednosne garancije.....</i>	<i>64</i>
	<i>Kontrola dokaza bezbednosne garancije.....</i>	<i>65</i>
	<i>Analiza dokaza bezbednosne garancije</i>	<i>65</i>
	<i>Argumentovanje bezbednosne garancije.....</i>	<i>65</i>
3.2.6	Nadzor bezbednosnog stanja	66
	<i>Analiza zapisa događaja</i>	<i>67</i>
	<i>Identifikovanje bezbednosnih incidenata</i>	<i>68</i>
	<i>Upravljanje reagovanjima na bezbednosne incidente.....</i>	<i>69</i>
	<i>Praćenje promena bezbednosnog stanja.....</i>	<i>69</i>
	<i>Nadzor kontrola zaštite</i>	<i>70</i>
	<i>Preispitivanje bezbednosnog stanja.....</i>	<i>70</i>
	<i>Zaštita artefakata monitoringa zaštite.....</i>	<i>71</i>
3.2.7	Specifikacija bezbednosnih potreba.....	71
	<i>Unapređenje razumevanja bezbednosnih potreba klijenata</i>	<i>72</i>
	<i>Identifikovanje primenjivih zakona, politika i ograničenja</i>	<i>72</i>
	<i>Identifikovanje bezbednosnog konteksta sistema</i>	<i>73</i>
	<i>Izrada opšte slike bezbednosnih operacija sistema</i>	<i>73</i>
	<i>Identifikovanje opštih bezbednosnih ciljeva.....</i>	<i>74</i>
	<i>Definisanje bezbednosnih zahteva</i>	<i>75</i>
	<i>Obezbeđivanje saglasnosti o bezbednosti</i>	<i>75</i>
3.2.8	Obezbeđivanje bezbednosnog ulaza	76
4	ZAKLJUČAK.....	77

PRILOG A. PRIMERI MERENJA ZAŠTITE INFORMACIJA (NIST).....	79
PRILOG B. PRIMERI MERENJA ZAŠTITE INFORMACIJA (ISO27k).....	81
PRILOG C. PRIMER KONSTRUKCIJE MERENJA (ISO/IEC)	82
PRILOG D. FUNKCIONALNA I INFORMACIONA IMOVINA SISTEMA.....	84
D-1 PRIMARNA IMOVINA	84
D-1.1 Poslovni procesi/podprocesi i aktivnosti	84
D-1.2 Primarne informacije	84
D-2 SREDSTVA ZA PODRŠKU.....	85
D-2.1 Hardver	85
D-2.1.1 Oprema za obradu podataka (aktivna)	85
D-2.1.2 Prenosiva oprema	85
D-2.1.3 Fiksna oprema	85
D-2.1.4 Periferna oprema.....	85
D-2.1.5 Pasivni medijumi	85
D-2.1.6 Elektronski medijumi.....	85
D-2.2 Softver	85
D-2.2.1 Operativni sistem.....	85
D-2.2.2 Softveri za održavanje ili administraciju	85
D-2.2.3 Standardni softver ili softverski paket	85
D-2.2.4 Poslovna aplikacija.....	86
Standardna poslovna aplikacija	86
Specifična poslovna aplikacija.....	86
D-2.3 Mreža.....	86
D-2.3.1 Medijumi i podrška	86
D-2.3.2 Pasivni ili aktivni relej.....	86
D-2.3.3 Komunikacioni interfejs.....	86
D-2.4 Personal.....	86
D-2.4.1 Donosilac odluke.....	86
D-2.4.2 Korisnik	87
D-2.4.3 Osoblje za operativni rad i održavanje.....	87
D-2.4.4 Programer.....	87
D-2.5 Lokacija.....	87
D-2.5.1 Spoljašnje okruženje	87
D-2.5.2 Prostor	87
D-2.5.3 Zona	87
D-2.5.4 Glavni servisi	87
D-2.5.5 Komunikacija	87
D-2.5.6 Pomoćna sredstva	87
D-2.6 Organizacija.....	88
D-2.6.1 Autoritet.....	88
D-2.6.2 Organizaciona struktura.....	88
D-2.6.3 Projektna ili sistemska organizacija	88
D-2.6.4 Podugovarači / Dobavljači / Proizvođači.....	88

PRILOG E. PRIMENA APLIKACIJE “APPRAISAL ASSISTANT” ZA	
UNAPREĐENJE PROGRAMA MERENJA ZAŠTITE	89
5 LITERATURA.....	98

PREGLED SLIKA

<i>Slika 1 Brze (jeftine) i spore (skupe) metrike</i>	<i>16</i>
<i>Slika 2 Sazrevanje programa zaštite informacija i tipovi merenja.....</i>	<i>19</i>
<i>Slika 3 Uspostavljanje programa metrike zaštite informacija.....</i>	<i>22</i>
<i>Slika 4 Veza između metrike zaštite i podataka</i>	<i>26</i>
<i>Slika 5 Uloge u organizaciji kojima se najčešće prezentuju metrike zaštite</i>	<i>29</i>
<i>Slika 6 Primeri metoda za prezentovanje metrike zaštite informacija.....</i>	<i>30</i>
<i>Slika 7 Primer korišćenja instrument tabli u metrikama zaštite informacija</i>	<i>32</i>
<i>Slika 8 Proces implementacije programa merenja zaštite informacija</i>	<i>34</i>
<i>Slika 9 Model merenja performansi zaštite informacija</i>	<i>41</i>
<i>Slika 10 Tokovi informacija između procesa upravljanja rizikom</i>	<i>51</i>
<i>Slika 11 Proces procene uticaja</i>	<i>52</i>
<i>Slika 12 Proces procene pretnji.....</i>	<i>55</i>
<i>Slika 13 Proces procene ranjivosti</i>	<i>58</i>
<i>Slika 14 Bezbednosni ulazi za identifikovanje ranjivosti</i>	<i>59</i>
<i>Slika 15 Proces procene bezbednosnog rizika.....</i>	<i>61</i>
<i>Slika 16 Bezbednosni ulazi za procenu uticaja realizacije izloženosti</i>	<i>62</i>
<i>Slika 17 Bezbednosni ulazi za procenu ukupne neodređenosti rizika izloženosti</i>	<i>62</i>
<i>Slika 18 Bezbednosni ulazi za prioritetizaciju rizika</i>	<i>63</i>
<i>Slika 19 Proces izgradnje bezbednosne garancije.....</i>	<i>64</i>
<i>Slika 20 Proces nadzora bezbednosnog stanja.....</i>	<i>67</i>
<i>Slika 21 Bezbednosni ulazi za praćenje promena bezbednosnog stanja.....</i>	<i>70</i>
<i>Slika 22 Proces specifikacije bezbednosnih potreba</i>	<i>72</i>
<i>Slika 23 Bezbednosni ulazi za izradu konceptualne arhitekture bezbednosti sistema</i>	<i>74</i>
<i>Slika 24 Bezbednosni ulazi za identifikovanje opštih bezbednosnih ciljeva.....</i>	<i>74</i>

PREGLED TABELA

<i>Tabela 1 Predmet istraživanja korišćenja metrike zaštite u praksi</i>	<i>10</i>
<i>Tabela 2 Karakteristike metrika zaštite informacija.....</i>	<i>13</i>
<i>Tabela 3 Primeri metrika zaštite prema kategorijama</i>	<i>14</i>
<i>Tabela 4 Pristup za izbor metrike – Odozgo na dole.....</i>	<i>23</i>
<i>Tabela 5 Pristup za izbor metrike – Odozdo na gore</i>	<i>23</i>
<i>Tabela 6 Najčešće potrebe pojedinih zainteresovanih strana</i>	<i>24</i>
<i>Tabela 7 Najčešće korišćene metrike zaštite informacija</i>	<i>25</i>
<i>Tabela 8 Izbor načina prezentovanja metrike zainteresovanim stranama.....</i>	<i>31</i>
<i>Tabela 9 Komparativna tabela rezultata.....</i>	<i>32</i>
<i>Tabela 10 Korišćenje tabele rezultata sa fokusom na standardne kontrole zaštite informacija</i>	<i>33</i>
<i>Tabela 11 Obrazac merenja zaštite informacija (NIST)</i>	<i>38</i>
<i>Tabela 12 Obrazac merenja zaštite informacija (ISO27k forum).....</i>	<i>38</i>
<i>Tabela 13 Generička konstrukcija merenja zaštite informacija (ISO/IEC)</i>	<i>39</i>
<i>Tabela 14 Primer primene modela merenja za dobijanje indikatora performansi kontrola zaštite</i>	<i>43</i>

1 METODOLOGIJA ISTRAŽIVAČKOG RADA

1.1 Uvodne napomene i obrazloženje rada

Metrika zaštite informacija je objektivna i kvantitativna analiza i interpretacija rezultata merenja performansi aktivnosti zaštite. Ne postoji jasna i opšta definicija metrike zaštite, ali je jasno da metrika zaštite treba da obezbedi objektivne i kvantitativne rezultate koji organizaciji daju uvid u efektivnost celokupnog programa zaštite informacija, kao i smernice za poboljšanje procesa zaštite. Poslednja faza ciklusa upravljanja sistemom zaštite informacija je preduzimanje korektivnih i preventivnih akcija za poboljšanje procesa zaštite, a puna primena metrike zaštite vidi se upravo u toj fazi.

Metrika zaštite informacija je disciplina u fazi razvoja, što dodatno otežava njenu primenu. Svi koji se danas bave razvojem programa metrike zaštite, mogu da se smatraju pionirima u toj oblasti i treba da prilagođavaju strategije metrike prema sopstvenom iskustvu i da kreativnošću odgovore na različite zahteve zainteresovanih strana.

Menadžeri zaštite informacija redovno nailaze na probleme dokazivanja isplativosti programa zaštite njihovih organizacija. Čak ni najbolje osmišljene prezentacije metrike zaštite ne ostavljaju utisak opravdanosti ulaganja u program zaštite. Jedan od primera komentara zainteresovane strane je: "Prezentacija je bila odlična, ali nisam video nikakve pokazatelje isplativosti ulaganja u program zaštite, ni kako da koristim rezultate metrike zaštite za upravljanje poslovanjem."

Proizvodi i sistemi zaštite dolaze na tržište posle dugotrajnog i skupog razvoja, sa evaluacijom ili bez evaluacije u praksi zaštite, a jedna od posledica je da korisnici postavljaju nerealne bezbednosne zahteve i definišu neadekvatne bezbednosne ciljeve. Samim tim, koncepti zaštite i tehnička rešenja arhitekture sistema zaštite ne odgovaraju stvarnom stanju rizika IKT sistema. Takođe, korisnici često servise zaštite *poverljivosti*, *integriteta* i *raspoloživosti* informacija, u praksi IKT zaštite, smatraju više teorijskim i „umetničkim“ aktivnostima, a implementiraju ih malobrojni eksperti za zaštitu, najčešće na ličnu inicijativu.

U svrhe ovog rada, za praktičnu primenu poboljšavanja procesa zaštite informacija, korišćen je softverski alat *Appraisal Assistant*, proizvod austrijskog instituta *Software Quality Institute* (SQI)¹, koji sadrži nekoliko standardnih modela procesa, ali ne i model procesa zaštite. Iz tog razloga, iskorišćena je opcija aplikacije koja omogućava dodavanje novog modela, što je u svrhe ovog rada i urađeno, te je aplikacija obogaćena modelom sazrevanja procesa zaštite informacija, koji je baziran na međunarodnom standardu ISO/IEC 21827.

1.2 Predmet istraživanja

Zaštita informacija u poslednjih nekoliko godina dobija sve viši prioritet u mnogim organizacijama. Troškovi za zaštitu informacija gotovo su obavezna komponenta budžeta, naročito u određenim sektorima – četvorostruko u odnosu na 2001. godinu. Iako je i dalje teško obezbediti da ovo pitanje dobije veći značaj kod glavnog rukovodstva, zaštita informacija sve više postaje centralna tačka, ne samo u pogledu ulaganja, već i u pogledu vraćanja uložених investicija.

¹ [Software Quality Institute, Griffith University](http://www.sqi.ac.uk/)

Suočavajući se sa izazovima narušavanja bezbednosti informacija, menadžeri zaštite se, više nego ikad, smatraju odgovornima i od njih se zahteva da demonstriraju efikasnost svojih programa zaštite. Metrike zaštite su ključna sredstva koja menadžerima zaštite stoje na raspolaganju kako bi odgovorili na ove izazove. Iz tog razloga, predmet istraživanja u ovom radu je potpunije i detaljnije određenje metrike zaštite informacija, njenih prednosti i mana, moguće primene i predlog programa metrike zaštite.

Predmet istraživanja fokusiran je na tri moguća tipa merenja performansi zaštite informacija:

1. Merenje implementacije zaštite, za utvrđivanje ispunjenja bezbednosnih zahteva;
2. Merenje efektivnosti i efikasnosti zaštite, za utvrđivanje rezultata aktivnosti zaštite;
- i
3. Merenje uticaja ili posledica bezbednosnih događaja na poslovanje.

1.3 Osnovna hipoteza

Danas većina organizacija svoj poslovni i informacioni sistem usaglašava sa standardnim preporukama za upravljanje zaštitom informacija. Najčešći cilj ovakvog usaglašavanja je da se prikaže poštovanje zakonskih i ugovornih zahteva za zaštitu ličnih i poslovnih informacija, da je obezbeđen kontinuitet poslovanja i da se posedovanjem sertifikata dobije dodatna konkurentnost i ugled na tržištu. Popularni sertifikacioni standard zaštite informacija ISO/IEC 27001 zahteva merenje efektivnosti implementiranih kontrola zaštite, redovnu proveru (*audit*) ispunjenosti zahteva standarda i preduzimanje akcija za poboljšanje sistema zaštite. Problem je što rezultati ovakvih provera ne nude dovoljnu meru performansi bezbednosnog uticaja na poslovanje, ne ocenjuju zrelost i kapacitete procesa zaštite, niti je na osnovu ovakvih provera moguće precizno utvrditi sve slabosti i prednosti koji su osnova za izradu akcionog plana poboljšanja zaštite.

Tipovi merenja performansi zaštite informacija (implementacija, efektivnost/efikasnost i uticaj), koji realno mogu da se primene i iskoriste za poboljšanje performansi zaštite, zavise od nivoa zrelosti procesa zaštite informacija. Dokumentovanjem i implementacijom bezbednosnih ciljeva i strateških planova, otvaraju se kapaciteti za sazrevanje procesa zaštite.

Kako se sistem zaštite informacija razvija, podaci performansi zaštite postaju sve dostupniji i konkretniji, a merenja se sve više fokusiraju na efektivnost/efikasnost programa zaštite informacija i operativne rezultate primene kontrola zaštite informacija. Što je više podataka dostupno, poteškoća merenja opada, a rastu kapaciteti za automatsko prikupljanje podataka.

1.4 Radna hipoteza

Rezultati merenja performansi zaštite su osnovni ulazni podaci za metriku zaštite informacija, zato je neophodno sistem upravljanja zaštitom informacija pojačati metričkim sistemima. Preduslov za izradu metrike zaštite informacija je da organizacija ima definisane procese zaštite, naročito one koji se bave upravljanjem bezbednosnim rizicima, koji treba da se izvršavaju paralelno sa ostalim podlovnim procesima. Pošto su se sada stvorili kapaciteti organizacije aktivnosti zaštite mogu da se izmere i postave u odnos sa ostalim poslovnim aktivnostima, što olakšava primenu metrike zaštite i potvrđuje opšte prihvaćeni princip upravljanja da se ne može upravljati aktivnostima koje ne mogu da se izmere.

Prilikom implementacije programa merenja performansi zaštite informacija primenjuju se sledeći principi:

- Merenja moraju da obezbede kvantitativne informacije (procenti, srednje vrednosti i numeričke vrednosti);
- Podaci koji su potrebni u merenjima moraju uvek biti dostupni;
- Samo ponovljivi pocesi zaštite informacija mogu biti uključeni u merenja; i
- Merenja moraju biti od koristi za praćenje performansi i usmeravanju resursa.

Da bi merenja bila korisna za poboljšanje performansi zaštite, neophodno je imati zrele procese zaštite i visok nivo zrelosti primene kontrola zaštite informacija. Tada se primarni fokus merenja pomera zajedno sa promenom nivoa zrelosti procesa zaštite i zrelosti primene kontrola zaštite informacija.

1.5 Ciljevi istraživanja

Osnovni cilj istraživanja je ispitivanje nivoa razumevanja i spremnosti organizacija za korišćenje metrika zaštite u praksi. Na spremnost organizacije da uloži u programe metrike zaštite direktno utiče nivo razumevanja prednosti od primene metrika zaštite u upravljanju poslovanjem. Sekundarni cilj rada je da menadžerima zaštite informacija, rukovodstvu i osoblju IT zaštite, izvršnom rukovodstvu i internim auditorima obezbedi uvid u najčešće probleme korišćenja metrika zaštite i praktične preporuke za njihovo prevazilaženje.

Osnovni cilj istraživanja je da se najvišem rukovodstvu i drugim zainteresovanim stranama ukaže da merenje performansi zaštite informacija zavisi od zrelosti njihovog sistema ili programa zaštite. Sekundarni cilj rada je prikupljanje i analiza standardnih obrazaca i mernih konstrukcija, da bi organizacija mogla da odabere model koji joj najviše odgovara.

Prema tome, drugi cilj ovog rada je prezentovanje efektivnih praksi metrike zaštite u preduzećima koja merenje svojih aktivnosti zaštite zaista shvataju ozbiljno.

1.6 Metodi istraživanja

U dokazivanju hipoteze korišćeni su analitičko–sintetički, komparativno–istorijski i deskriptivni metodi istraživanja. Celokupan rad je koncipiran kao analitičko–istraživački. Rezultati istraživanja su preispitani; analizirana je i definisana metrika zaštite informacija; izrađen je program merenja performansi zaštite informacija; identifikovane su prednosti i glavni problemi korišćenja metrika zaštite u praksi i izrađen je predlog rešenja; odabrani su najaktuelniji modeli primene merenja performansi zaštite informacija; za evaluaciju i poboljšanje procesa zaštite informacija iskorišćen je softverski alat *Appraisal Assistant*.

Za prezentovanje primene metrike u zaštiti informacija iskorišćeni su rezultati istraživanja specijalizovane interesne grupe ISF² i njenih članica, koji su izrađeni na osnovu:

- Internet istraživanja;
- Diskusija o ključnim pitanjima na devet konferencija: Štokholm, Frankfurt, London (dva puta), Brisel, Cape Town, Singapur, Melburn i Boston;
- Zapažanja 129 učesnika konferencija;
- Prezentacija 11 članica ISF foruma;
- Analiza 56 anketa na temu metrike zaštite; i
- Intervjua sa 12 članica ISF foruma, njihova iskustva i razumevanje metrika zaštite.

² Information Security Forum www.securityforum.org

Osnovni problemi kod korisnika metrike u zaštiti informacija ustanovljeni su korišćenjem trokomponentnog modela istraživanja: (Odgovori na ova pitanja dati su u Tabela 1.)

- **Zašto** se koristi metrika zaštite (cilj metrike)?
- **Šta** metrika zaštite koristi (prikupljanje ulaznih podataka)?
- **Kako** se koriste i prezentuju metrike zaštite informacija (strategija primene i način prezentovanja rezultata metrike)?

Tabela 1 Predmet istraživanja korišćenja metrike zaštite u praksi

Komponente modela istraživanja	Primeri iz prakse	Osnovni problemi u praksi
Zašto se koristi metrika zaštite	• izveštavanje rukovodstva • prikazivanje usklađenosti sa standardnim, zakonskim i ugovornim zahtevima za zaštitu informacija • podrška aktivnostima upravljanja rizicima	• bez jasne primene • poteškoće da se metrike zaštite stave u odnos sa poslovanjem • nekompatibilnost metrika zaštite sa poslovnim metrikama
Šta metrika zaštite koristi i prikuplja	• incidenti • zaštita od virusa • upravljanje rizicima • upravljanje pečovima • usklađenost sa internim politikama • nalazi <i>audit</i>-a • troškovi	• poteškoće u izboru metrike zaštite • premalo, na visokom nivou, poslovno orjentisanih metrika zaštite • nedostatak poslovnog aspekta bezbednosti informacija
Kako se metrike koriste i prezentuju	• prezentovanje različitim zainteresovanim stranama • prezentovanje na različite načine	• poteškoće u identifikovanju pravih zainteresovanih strana • poteškoće u izboru odgovarajuće forme prezentovanja • neprecizno opisivanje bezbednosnog stanja

2 PRIMENA METRIKE U CILJU POBOLJŠAVANJA PROCESA ZAŠTITE INFORMACIJA

*Ono što ne možeš izmeriti, ne možeš ni poboljšati.*³

Zaštita informacija je oblast upravljanja koja nema dobro definisane tehnike merenja. U logistici, metrike poput “transportovani tovar po kilometru” ili “održavanje inventara u magacinu” prikazuju efikasnost prevoza i stanje skladišta. U finansijama postoji merna tehnika za određivanje vrednosti rizika, koja se bazira na hronologiji padova cena i koristi se za projektovanje finansijskih gubitaka, dok u zaštiti informacija još uvek ne postoji konsenzus oko ključnih indikatora. Nedostatak konsenzusa uglavnom potiče od generalnog mišljenja da je sramota biti prepoznatljiv po bezbednosnim događajima. Organizacije koje su doživele hakerski napad, nerado iznose svoje bezbednosne incidente u javnost, a ako ih nisu imale, ne hvale se, jer ne žele da motivišu napadače i izazivaju sudbinu svoje *firewall* zaštite.

Zaštita informacija je upravljačka disciplina koja se sastoji od niza analitičkih ispitivanja. Prilikom usklađivanja troškova kontrola zaštite sa potencijalnim gubicima od procenjenih rizika, odluka će se lakše doneti kada postoji metrika. Ispravno merenje zavisi od razumevanja zahteva zainteresovanih strana. U medicini, doktor će pitati “kakvo je zdravstveno stanje pacijenta.” U zdravstvenom sistemu, pitanje će glasiti “koliko pacijenata boluje od određene bolesti i na koji način su oboleli.” U zaštiti informacija postavljaće se pitanja:

- *Koliko je naš program zaštite efektivan?*
- *Da li je bezbednost na višem nivou nego prošle godine?*
- *Kako možemo da se uporedimo sa ostalim organizacijama u pogledu zaštite informacija?*
- *Da li smo dovoljno bezbedni?*
- *Da li smo dovoljno uložili u zaštitu?*
- *Koje su nam opcije za transfer rizika?*

Radi lakšeg razumevanja pojma “metrika” dobro je znati razliku između metrike i merenja.

Merenje daje trenutni uvid u status određenih aktivnosti, dok je metrika izvedena kombinacijom preseka unapred odabranih rezultata dva ili više merenja izvršenih u različito vreme. Merenja se vrše izračunavanjem, a metrike su proizvod analize. Drugim rečima, rezultati merenja su objektivni i sirovi podaci koji mogu automatski da se generišu, dok su metrike objektivne ili subjektivne interpretacije tih podataka, [14].

Merenje daje jednokratni uvid u specifične merne parametre sistema zaštite, a metrika je višekratno merenje u dužem vremenskom periodu ili sredstvo za interpretaciju agregiranih mernih podataka na višem nivou, [12].

Merenja zaštite informacija mogu da se ostvare na različitim nivoima organizacije. Detaljna merenja i prikupljanje podataka na nivou informacionog sistema mogu biti agregirana i progresivno podignuta na više nivoe, sistemske ili programske, zavisno od veličine i kompleksnosti organizacije, [6].

³ [Lord Kelvin](#)

Merenje podrazumeva skup aktivnosti prikupljanja, analize i prezentovanja sirovih podataka objekata merenja zaštite informacija, dok metrika predstavlja objektivne ili subjektivne interpretacije tih podataka, [11].

Metrika zaštite informacija se koristi da pomogne u donošenju odluka i za poboljšanje performansi i kontrolisane odgovornosti, putem prikupljanja, analize i prezentovanja mernih podataka, [5].

Svrha metrike zaštite informacija je da se na osnovu mernih rezultata kontroliše status izmerenih aktivnosti i doprinese njihovom poboljšanju primenom korektivnih akcija, [9].

Razne publikacije, knjige i standardi unose zabunu zbog različitih definicija metrike bezbednosti. Ove definicije nisu opšte prihvaćene i mogu izazvati konfuziju. Neke od ovih definicija metrike zaštite informacija su:

Metrike zaštite će dati korisne informacije samo ako ispunjavaju taktičke i strateške ciljeve za performansama zaštite informacija, koji mogu lako da se prikupe i izmere. Takođe, rezultati metrike moraju biti ponovljivi, sa relevantnim pregledom trendova i da budu korisni za praćenje rada i upravljanje resursima, [11].

Metrika zaštite informacija je definisan način merenja (metod merenja, računska operacija, analitički model), ili merilo jednog ili više atributa merenja, [9].

Metrika zaštite kvantitativnim, statističkim i/ili matematičkim analizama meri funkcionalne troškove zaštite, korist, uspehe, otkaze, promene i uloženi trud u očuvanje zahtevanog stanja bezbednosti, [7].

Merenja zaštite informacija su bazirana na strateškim i taktičkim ciljevima performansi zaštite informacija, [5]. Ciljevi performansi zaštite informacija formulišu informacione potrebe⁴, npr. "Svi zaposleni moraju da imaju adekvatnu obuku za razvoj svesti o potrebi zaštite informacija," i da su usmereni ka ispunjenju cijeva politika i procedura zaštite informacija koje regulišu konzistentnost implementacije kontrola zaštite informacija na nivou cele organizacije. Primeri ispunjenih ciljeva performansi zaštite informacija su:

- Svi novi zaposleni su prošli obuku za zaštitu informacija;
- Obuka zaposlenih uključuje pravila ponašanja; i
- Izvođenje buke podrazumeva upoznavanje zaposlenih sa politikama i procedurama zaštite informacija.

Provera da merenje zaštite informacija ispunjava strateške i taktičke ciljeve vrši se:

- Kvantifikovanjem implementacije, efikasnosti i efektivnosti kontrola zaštite;
- Analizom adekvatnosti izvršavanja aktivnosti programa zaštite informacija; i
- Identifikovanjem mogućih akcija za unapređenje.

U toku razvoja merenja zaštite informacija identifikuju se i prioritetizuju strateški i taktički ciljevi, kao i zakonski i ugovorni zahtevi za merenje performansi zaštite informacija koji odgovaraju operativnim prioritetima organizacije.

Aktivnosti zaštite informacija koji mogu dati podatke za merenje mogu biti rezultati procene rizika, testiranja proboja, audita zaštite i monitoringa. Rezultati procene

⁴ Informacije neophodne za upravljanje strateškim i taktičkim ciljevima, rizicima i problemima. Svrha merenja zaštite informacija.

efektivnosti programa obuke i razvoja svesti o potrebi zaštite, takođe mogu da se kvantifikuju i koriste kao izvori podataka za merenja.

2.1 Osnovna podela metrike u zaštite informacija

Metrike zaštite se dele na one koje se koriste za kvantitativno vrednovanje (provera ispravnosti mehanizama zaštite) i one koje se koriste za merenje performansi (za kontinualno poboljšanje procesa zaštite).

Postoje dva fundamentalna tipa metrike zaštite informacija: *rezultatski orjentisana metrika* i *metrika sazrevanja procesa zaštite*:

- Rezultatski orjentisana metrika koristi se za smanjenje troškova, povećanje prihoda, povećanje produktivnosti, smanjenje proizvodnog ciklusa i smanjenje rizika od prekida poslovanja.
- Metrika sazrevanja procesa zaštite ima za cilj da poboljša upravljačke, organizacione i tehničke procese zaštite.

Iako se čini da su ove dve metrike slične, metrika sazrevanja procesa zaštite fokusira se na **efektivnost**, a tipična pitanja na koja daje odgovor su:

- *Da li je proces unapređen?*
- *Da li proces daje željene rezultate?*
- *Da li proces izlazi van utvrđenog područja primene?*

Većina rukovodstva na metrike zaštite informacija gledaju “mikroskopski”, sa ciljem da eliminišu aktivnosti koje ne daju nikakvu poslovnu vrednost, a ne da ih unaprede.

Razvijeno je više metrika za merenje zrelosti procesa zaštite i upravljanje programom zaštite informacija, kao što su: *SSE–CMM⁵ (ISO/IEC 21827)*, *INFOSEC IA–CMM⁶*, *IS Program Maturity Grid* i *SW Security Metrics*, [12].

2.1.1 Karakteristike i značaj metrike u zaštiti informacija

Sve metrike zaštite informacija imaju definisane karakteristike. Neke od karakteristika metrika zaštite informacija date su u Tabela 2.

Tabela 2 Karakteristike metrika zaštite informacija

Karakteristike	Komentar
Naziv	Razumljiv naslov ili naziv koji opisuje metriku
Namena	Čemu služi metrika
Cena	Procena stvarnih troškova prikupljanja i obrade podataka za izradu metrike
Tip	Kakva je vrsta metrike, na primer: tehnička ili upravljačka, savremena ili zastarela, numerička ili tekstualna
Lokacija	Mesta gde: • mogu da se prikupe podaci za metriku zaštite • se nalaze podaci korišćeni u prethodnim metrikama • su primenjene prethodne metrike zaštite
Frekvencija	Koliko često treba: • prikupljati podatke • prezentovati metriku zaštite

⁵ Security System Engineering Capability Maturity Model

⁶ INFOSEC Assessment - Capability Maturity Model

Karakteristike	Komentar
Kategorija	Kategorije metrike zaštite mogu biti: • broj pojave određenih događaja (broj) • ponavljanje događaja (frekvencija) • vreme utrošeno na događaj (trajanje) • troškovi događaja (cena)
Start/stop kriterijum	Kriterijum za pokretanje i prekidanje: • prikupljanja podataka za metriku • upotreba i prezentovanje metrike
Trajanje prikupljanja	Utvrđivanje vremenskog perioda potrebnog za prikupljanje podataka
Period upotrebe	Procena vremenskog perioda u kom će se koristiti rezultati metrike

Definisanje karakteristika metrike omogućava konzistentnost njenog korišćenja, izbor, komparaciju i analizu.

I pored navedenih prednosti, u praksi se uglavnom ne određuju karakteristike metrike zaštite.

U Tabela 3 navedene su četiri generičke kategorije metrike zaštite (*broj, frekvencija, trajanje i cena*) sa primerima merenja.

Tabela 3 Primeri metrika zaštite prema kategorijama

Kategorija	Primeri
Broj (koliko puta se nešto dogodilo)	Broj: • bezbednosnih događaja • blokiranih poslovnih <i>e-mails</i> • izvršenih bekapovanja • nove informacione imovine • propusta osoblja odgovornih za zaštitu • sprečavanja korišćenja osetljivih dokumenata • sprečavanja korišćenja zaštićenih aplikacija
Frekvencija (koliko često se nešto događa)	Frekvencija: • incidenata • revizije dokumenata • dodele privilegija • <i>audit-a</i> kontrole pristupa • pristupanja web sajtovm • bekapovanja servera • fizičkih pristupa server sali
Trajanje (koliko dugo je trajao događaj)	Trajanje: • incidenta • bekapovanja • izloženosti pretnjama • rešavanja incidenta • pečevanja • oporavljanja • monitoringa

Kategorija	Primeri
Cena (koliki su gubici zbog događaja)	Cena: • rešavanja događaja ili zamene oštećene imovine • saniranja incidenta • vraćanja u prethodno stanje (oporavak) • kontrola zaštite • administracije • sudskih procesa • edukacije

Najčešći primeri metrika zaštite informacija su:

- Određivanje efektivnosti kontrola zaštite;
- Broj incidenata u datom vremenskom periodu; i
- Performanse zaštite u odnosu na budžet.

Teoretski, metrike zaštite informacija treba da daju kvantitativne, konzistentne i ponovljive rezultate. Metrike zaštite moraju da obezbede osnovu za:

- Analizu efektivnosti programa zaštite;
- Izveštavanje rukovodstva;
- Razumevanje na koji način treba održavati bezbednost informacija; i
- Demonstraciju vrednosti zaštite informacija za poslovanje.

Za još bolje razumevanje metrike u zaštiti informacija, potrebno je znati razlikovati dobre od loših metrika, kao i njihove nedostatke i prednosti za organizaciju.

Dobre metrike zaštite informacija

Često se kaže da su dobre metrike one koje su određene, merljive, primenjive, ponovljive i vremenski nezavisne. Metrike zaštite informacija su korisne ako pokazuju stepen ispunjenja bezbednosnih ciljeva, npr. zaštite tajnosti podataka, i ako usmeravaju akcije za unapređenje celokupnog programa zaštite. Dobre metrike treba da budu:

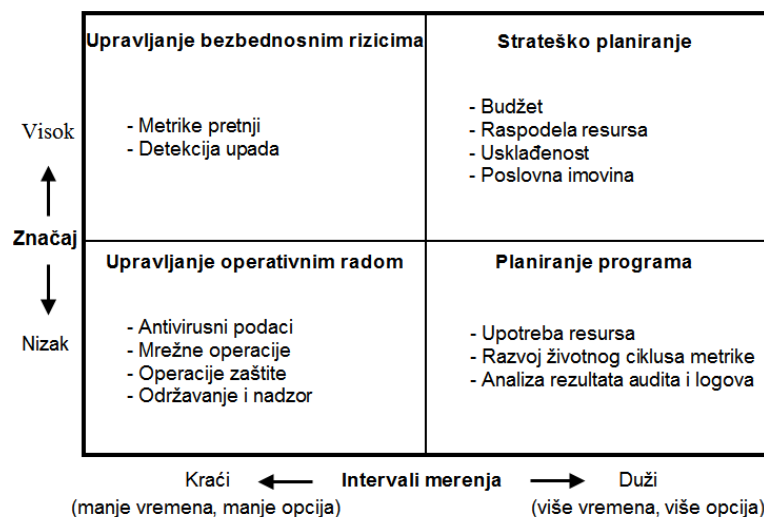
1. Konzistentne – bez subjektivnih kriterijuma

- o Metrike su kredibilne samo ako se izvode na konzistentan način. Ko god da primenjuje utvrđen metod i koristi iste merne podatke, treba da dobije iste rezultate. Metrike koje zavise od subjektivnih mišljenja, uopšte nisu metrike, nego procene. Dobru metriku je jednostavno testirati, dovoljno je samo dvema različitim osobama prezentovati istu metriku, pa proveriti da li su im zaključci jednaki.

2. Rentabilne – da se podaci prikupljaju automatski gde god je to moguće

- o Svaka metrika zahteva izvesno vreme izrade. Izrada metrike polazi od prikupljanja sirovih podataka i završava sa korisnim analitičkim računima. Što znači, da neko ili nešto treba da prikupi podatke, ako je potrebno i da ih transformiše u drugi oblik, pa da ih obradi i formatira u jasne rezultate. Neke metrike ove korake izvršavaju odjednom, u brzom procesu (jednostavan SQL upit ili API poziv metode) izvlačenja i prezentovanja korisnih informacija, dok druge metrike zahtevaju intervjuisanje, telefoniranje i korišćenje komparativnih tabela rezultata. Neefikasni metodi prikupljanja podataka oduzimaju dragoceno vreme, a ono se može smanjiti boljim planiranjem programa metrike zaštite informacija.
- o Za mnoge metrike procesa zaštite postoji pravilo da je “često” bolje nego “po nekad,” kao što je slučaj kod procesa upravljanja bezbednosnim

rizicima ili operativnim radom. Metrike izrađene na osnovu podataka dobijenih sa kratkim intervalima uzorkovanja (na dnevnom ili nedeljnom nivou) pomažu u analizi efektivnosti aktivnosti zaštite, za razliku od metrika zasnovanih na rezultatima godišnjeg preispitivanja sistema zaštite. Ako se metrika često izvodi, onda je prikupljanje podataka jeftinije i brže, kao što je ilustrovano na Slika 1, [1].



Slika 1 Brze (jeftine) i spore (skupe) metrike

- o Pre donošenja odluke o kreiranju metrika zasnovanih na uzorcima na dnevnom ili nedeljnom nivou, treba se dobro zapitati da li je to izvodljivo, ili razmotriti metode za ubrzavanje procesa merenja. Kao i u slučaju konzistentne metrike, kriterijum da dobra metrika bude jeftina najlakše će biti zadovoljen ako se podaci za metriku prikupljaju automatski.
3. **Izražene u brojevima ili procentima** – ne u kvalitativnim procenama, poput visok, srednji, nizak
- o Dobre metrike treba da budu izražene u brojevima ili procentima. Pod brojem, ovde se podrazumeva kardinalni broj (brojnost), koji pokazuje koliko nečega ima, za razliku od ordinalnih brojeva koji označavaju poziciju. Na primer, broj defekata zaštite izražen u kardinalnom broju daje kvantitativnu meru defekata, dok subjektivne procene *visoko-srednje-nisko* (ordinalni brojevi 1, 2 i 3) predstavljaju relativne nivoe, a ne tačne numeričke ili procentualne pokazatelje performansi.
 - o Metrike koje nisu kvantitativne, ne kvalifikuju se kao dobre metrike. Na primer, “semafori” (crveno-žuto-zeleno) nisu dobre metrike i nemaju merne jedinice. Semafori se obično koriste u prezentacijama koje su orjentisane za donošenje strateških odluka, ali samo kao podrška numeričkim podacima ili skretanje pažnje na značajna odstupanja od ciljeva zaštite. Ako metrike već imaju precizne pokazatelje, onda ih ne treba uopštavati semaforima.
4. **Izražene u mernim jedinicama** – defekti, vreme, novac,....
- o Rezultati metrike, pored numeričkih vrednosti, treba da budu izraženi u mernim jedinicama. Na primer, metrika “broj defekata zaštite” kao mernu jedinicu koristi *defekt*. Merne jedinice pomažu analitičarima da konzistentno predstave rezultate merenja defekata svih procesa.

- Često je bolje koristiti više mernih jedinica nego samo jednu. Jedna merna jedinica, kao što je “broj defekata zaštite,” ne može da se postavi u odnos sa svim drugim zahtevima, zato uvek važi pravilo da su dve merne jedinice bolje od jedne. Na primer, metrika “broj bezbednosnih rupa aplikacije na 1000 linija koda” nudi dve mere. Uključivanjem druge dimenzije (deljenje sa 1000 linija koda), proizvedena je metrika koja može da se koristi za *benchmarking* (merilo – indikator progressa performansi).
- 5. **Kontekstualne** – *idealno je da metrike ne odstupaju od konteksta, odnosno, da budu dovoljno relevantne za donošenje odluka o preduzimanju akcija za unapređenje celokupnog programa zaštite informacija.*
 - Metrike zaštite treba da se odnose na ono što se traži od njih. Na primer, da prezentuju infrastrukturu iz ugla kontrola zaštite, hronologiju kontinualnog poboljšavanja kontrola, ili da demonstriraju doprinos zaposlenih u sistemu zaštite. Nije obavezno da sve metrike budu specifične, ali specifičnost omogućava da svaka metrika bude usmerena na određenu zainteresovanu stranu koja će ove rezultate koristiti za donošenje odluka.
 - Kontekstualna metrika je od koristi zainteresovanim stranama. Na primer, metrika “srednja vrednosti napada na nivou cele organizacije” nikoga neće podstaći da bolje radi svoj posao, osim u slučaju da se na taj način indirektno traži veći budžet za program zaštite. Prema tome, ograničavanje metrike na određenu poslovnu aktivnost, npr., usluge elektronske trgovine, mnogo je efikasnije, jer može da se koristi u kontekstu specifičnom za donošenje odluka koje se odnose na zaštitu ovih servisa i odgovorno osoblje.

Loše metrike zaštite informacija

Dobre metrike podstiču diskusiju i analizu, a loše metrike uglavnom izazivaju negodovanje. Na svim diskusijama o metrikama zaštite uvek se vešto nameću standardni okviri za upravljanje zaštitom informacija, npr. ISO/IEC 27001, koji skreću pažnju sa mnogo važnijih pitanja, kao što su merenje procesa zaštite i ključni indikatori performansi.

Jedna od čestih zabluda je korišćenje taksonomija zaštite kao osnovu za program metrike zaštite. Većina opšte prihvaćenih metrika fokusira se na subjektivnim procenama u odnosu na uspostavljene taksonomije zaštite. Većina ovih metodologija koristi ISO/IEC 27001 okvir zaštite, koji definiše strukturni pristup upravljanja zaštitom informacija. Na primer, firma *Espiria* nudi rešenje za procenu zaštite i usluge *benčmarkinga*, u odnosu na ovaj standard. *Symantec* je razvio alat za kvantifikovanje rizika koji se bazira na ALE⁷ metodi.

Da ne bude zabune, ISO/IEC 27001 je odličan osnov za uspostavljanje sistema zaštite informacija, ali je loš za izradu programa metrike. Program metrike zaštite treba da se zasniva na ključnim indikatorima koji će kvantifikovati aktivnosti zaštite, a ne na taksonomijama, gde samo mogu da se dobiju odgovori “da” ili “ne” (tipični odgovori koji se traže prilikom provere da li organizacija ispunjava zahteve sertifikacionih standarda).

Značaj metrike zaštite informacija za organizaciju

Opšte prihvaćeni princip upravljanja glasi „Ne može se upravljati aktivnostima koje ne mogu da se izmere”.

Metrike mogu biti efektivan alat menadžera zaštite za utvrđivanje efektivnosti različitih komponenta programa zaštite, zaštite određenih sistema, proizvoda ili procesa, kao i

⁷ [Annual Loss Expectancy](#)

sposobnosti osoblja ili odeljenja da identifikuju bezbednosne probleme u domenu svojih odgovornosti za zaštitu informacija.

Metrike takođe pomažu u identifikovanju nivoa rizika zbog nepreduzimanja datih akcija, čime direktno usmeravaju aktivnosti prioritetizacije korektivnih akcija. Takođe, metrike mogu da se koriste za unapređenje bezbednosne svesti zaposlenih, [1], [9].

1. **Prednosti** korišćenja metrike zaštite informacija za organizaciju su brojne:
 - o Poboljšanje kontrolisane odgovornosti (accountability) ukazivanjem na specifične kontrole koje nisu implementirane ili su nekorektno implementirane;
 - o Merenje svakog aspekta sistema zaštite, kvantifikovanjem i korišćenjem različitih rezultata, kao što su rezultati analize rizika, testiranja sistema zaštite na proboj, testiranja bezbednosti informacija i evaluacije sistema i aktivnosti zaštite;
 - o Izolovanje problema u zaštiti u cilju opravdanja i usmeravanja investicija na oblast zaštite koju treba poboljšati;
 - o Usklađivanje sa zakonima i regulativama i angažovanje na proaktivnoj zaštiti;
 - o Opravdanje investiranja u program zaštite na bazi kvantitativnih mernih rezultata;
 - o Merenje efektivnosti implementiranih kontrola procesa/procedura zaštite, itd.
2. **Nedostaci** metrike su poznati. Glavni problem je merenje uticaja ljudskog faktora na sistem zaštite. Neke organizacije ga prevazilaze angažovanjem nezavisnih stručnjaka, pa nemaju potrebu za merenjem uticaja ljudskog faktora. Uzroci slabe ili neadekvatne implementacije metričkih sistema, generalno najčešće nastaju zbog nedostatka ili nepostojanja:
 - o Jasno definisanih procesa metričkih sistema;
 - o Svesti o potrebi kvalitetnog upravljanja zaštitom informacija;
 - o Spremnosti rukovodeće strukture za angažovanja u oblasti zaštite;
 - o Dokumenta zaštite (*Uputstvo za metriku zaštite*);
 - o Odgovornosti za sistem zaštite i
 - o Tehničkih rešenja metričkih sistema zaštite informacija, [12].

2.1.2 Glavni razlozi za korišćenje metrike u zaštiti informacija

Rezultati istraživanja pokazuju da su osnovni razlozi za korišćenje metrika u zaštiti informacija:

- Upravljanje sistemom zaštite informacija;
- Dodatne informacije u izveštajima za rukovodstvo;
- Usklađivanje sa zakonima, regulativama i standardima;
- Prikazivanje efikasnosti i efektivnosti zaštite u odnosu na zadate ciljeve;
- Demonstracija uticaja i značaja zaštite informacija za organizaciju;
- Podrška procesu procene rizika kao dobro usvojenom pristupu zaštite informacija;
- Dodatne informacije za upravljanje aktivnostima zaštite;
- Ukazivanje na prednosti i nedostatke sistema zaštite; i
- Predstavljanje nivoa bezbednosti informacija u odnosu na konkurenciju.

Metrike zaštite informacija najčešće se odnose na usklađenost sa zakonskim zahtevima, demonstraciju koristi od zaštite informacija za organizaciju i merenje efikasnosti i efektivnosti kontrola zaštite informacija.

Većina kompanija specijalizovanih za zaštitu informacija tvrdi da broj uspešnih proboja zaštite nije dovoljno merilo stanja bezbednosti informacija. Poznato je da sreća uvek igra veliku ulogu, ali nije poznato kako se meri sreća?! Iz tog razloga, pored zapisa o bezbednosnim incidentima, menadžer zaštite mora da posmatra i druge pokazatelje snage zaštite. Dodatna komplikacija koju rukovodioci zaštitom informacija moraju imati u vidu je definisanje primenjive metrike i izrada programa merenja zaštite informacija.

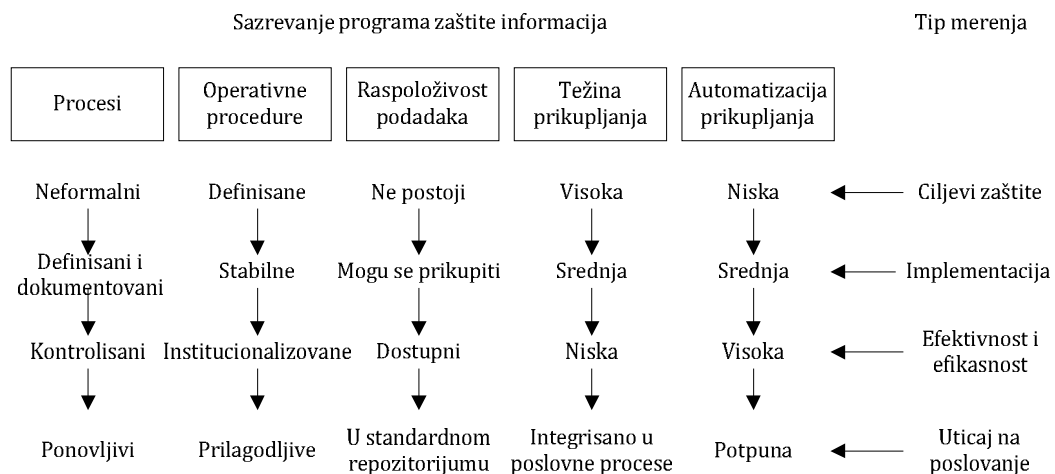
2.2 Tipovi merenja i njihova zavisnost od zrelosti programa zaštite informacija

Program zaštite informacija je sve što neka organizacija čini da uspostavi, primeni, kontroliše i unapredi bezbednost sistema, [12]. Zrelost programa zaštite informacija je definisana egzistencijom i institucionalizacijom procesa i procedura zaštite, [5].

Zrelost programa zaštite informacija određena je tipovima merenja koja mogu uspešno da se primene. Kako program zaštite informacija sazreva, njegove politike postaju detaljnije i bolje dokumentovane, procesi postaju standardniji i ponovljiviji, a celokupan program zaštite nudi veću količinu podataka koja mogu da se iskoriste za merenje performansi zaštite.

Kako je ilustrovano na Slika 2, da bi bilo moguće efektivno implementirati merenje, manje zreli programi prvo moraju razviti svoje strateške i taktičke ciljeve.

Zreliji programi koriste merenja za evaluaciju performansi, dok najzreliji programi koriste merenje efektivnosti/efikasnosti i poslovnih uticaja za utvrđivanje efekata njihovih procesa i procedura.



Slika 2 Sazrevanje programa zaštite informacija i tipovi merenja

Automatizacija prikupljanja podatka zavisi od raspoloživosti podataka u automatizovanim izvorima (baze podataka, liste, logovi,...). Prikupljanje mernih podataka se smatra potpuno automatizovanim kada su svi podaci prikupljeni bez učešća ili intervencija ljudi. Manuelno prikupljanje podataka uključuje upitnike, intervjuisanje i anketiranje osoblja.

Iako različiti tipovi merenja mogu da se istovremeno koriste, primarni fokus merenja zaštite informacija se pomera kako sazreva implementacija programa zaštite informacija.

Kad se zaštita informacija integriše u ostale procese organizacije i procesi zaštite informacija postanu ponovljivi, prikupljanje mernih podataka biće potpuno automatizovano, pa se uticaj bezbednosnih aktivnosti i događaja na poslovanje može utvrditi analizom i korelacijom mernih podataka. PRILOG A navodi primere merenja implementacije, efektivnosti/efikasnosti i uticaja.

2.2.1 Merenje implementacije

Merenje implementacije se koristi za prezentovanje progressa implementacije programa zaštite informacija, specifičnih kontrola, politika i procedura zaštite informacija, na primer, *procenat servera u sistemu sa standardnom konfiguracijom* ili *procenat informacionih sistema sa politikama lozinki konfigurisanim prema zahtevima*. Rezultati ovih merenja mogu biti manji od 100%, ali, kako program zaštite informacija, politike i procedure sazrevaju, rezultati mogu dostići i ostati na 100%. Od ove tačke, organizacija treba da krene sa merenjem efektivnosti/efikasnosti i uticaja.

Nikada se ne sme u potpunosti prekinuti sa merenjem implementacije, zato što ova merenja efektivno ukazuju na specifične kontrole zaštite kojima se vrši unapređenje.

2.2.2 Merenje efektivnosti/efikasnosti

Merenje efektivnosti/efikasnosti se koristi za proveru da li su procesi i kontrole zaštite korektno implementirani i da li ispunjavaju svoju namenu i bezbednosne zahteve. Na primer, *procenat ranjivosti operativnih sistema koji su otklonjeni pečevima ili na neki drugi način ublaženi* predstavlja merenje implementacije i efektivnosti. Na ovaj način meri se implementacija *Flaw Remediation (SI-2)* SP 800-53 preporučene kontrole zaštite, zato što rezultati merenja demonstriraju da li su ili nisu smanjene ranjivosti pomoću pečeva ili nekih drugih sredstava, a istovremeno, rezultati prikazuju efektivnost kontrole zaštite *Security Alerts and Advisories (SI-5)*, zato što svi rezultati koji su manji od očekivanih ukazuju na nedostatak mogućnosti prijema alarma i njihovog korišćenja za uspešno smanjenje ranjivosti, [2].

Merenje efektivnosti/efikasnosti odnosi se na dva aspekta rezultata implementacije kontrola zaštite: rezultati koji se odnose na **efektivnost** i vremenske raspodele rezultata koji se odnose na **efikasnost**. Na primer, merenje **efektivnosti** “*procenat bezbednosnih incidenata prouzrokovanih loše konfigurisanim kontrolama pristupa*” zasniva se na informacijama koje se odnose na implementaciju i **efektivnost** sledećih kontrola zaštite: *Incident monitoring (IR-5)*; *Audit Monitoring, Analysis, and Reporting (AU-6)*; i *Monitoring Configuration Changes (CM-4)*.

Pored toga, merenje **efikasnosti** “*procenat komponenti sistema koje se redovno održavaju*” zasniva se na informacijama koje se odnose na **efikasnost** sledećih kontrola zaštite: *Periodic Maintenance (MA-2)* i *Life Cycle Support (SA-3)*.

Merenja efektivnosti/efikasnosti donosiocima odluka daju ključne informacije o rezultatima rada prethodno donesenih odluka i politika. Ova merenja mogu dati uvid u poboljšanje performansi programa zaštite informacija. Pored toga, rezultati ovih merenja mogu da se koriste za kontinualni nadzor, jer pomažu u određivanju efektivnosti kontrola zaštite. Rezultati merenja efektivnosti/efikasnosti mogu da se koriste za utvrđivanje da li odabrane kontrole zaštite pravilno funkcionišu i doprinose lakšoj prioritizaciji korektivnih akcija.

2.2.3 Merenje uticaja

Merenje uticaja služi za prezentovanje uticaja bezbednosti informacija na ostvarenje misije organizacije. Ova merenja su specifična za organizaciju, pošto svaka organizacija ima

svoju jedinstvenu misiju. U zavisnosti od misije organizacije, merenje uticaja može da se koristi za kvantifikovanje:

- Troškova programa zaštite informacija ili bezbednosnih događaja;
- Stepenu poverenja u organizaciju stečenog programom zaštite informacija; ili
- Drugih uticaja zaštite informacija koji se odnose na misiju.

Ova merenja kombinuju informacije rezultata implementacije kontrole zaštite sa različitim informacijama o resursima. Ona mogu dati mnogo direktniji uvid u značaj zaštite informacija za organizaciju, što je korisno za izvršne direktore. Na primer, *procenat budžeta informacionog sistema određen za zaštitu informacija* zasniva se na informacijama koje se odnose na implementaciju, efektivnost i rashode SP 800-53 kontrole zaštite: *Allocation of Resources (SA-2)* i *Acquisitions (SA-4)*.

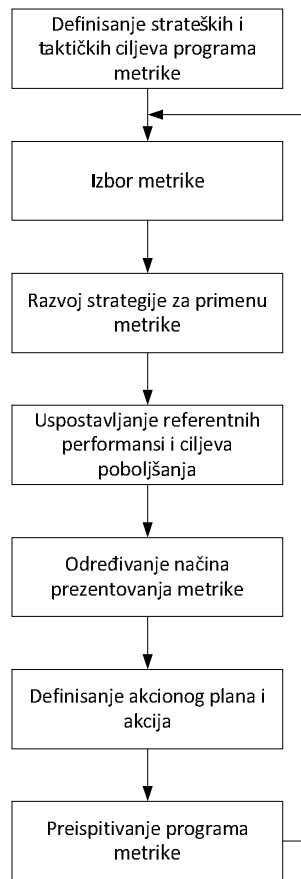
2.3 Uspostavljanje programa merenja zaštite informacija

Prilagođavanjem programa metrike zaštite postojećem okviru poboljšavanja procesa organizacije, postiže se lakše prihvatanje i razumevanje svih nivoa metrike. Na primer, kompanija *Dupont Corporation* svoj program metrike zasniva na popularnom procesu eliminisanja defekata "*Six Sigma Breakthrough Strategy*"; *First Union Corporation* svoj program metrike veže za usklađenost sa korporativnim standardima zaštite, dok kompanija *Bear, Stearns and Company* primenjuje *audit* pristup za verifikovanje usklađenosti sa industrijskim standardima kontrole zaštite i internim praksama zaštite, [14].

Bez obzira na postojeći okvir upravljanja procesima u organizaciji, za proces uspostavljanja programa metrike zaštite dovoljno je slediti sledećih sedam koraka:

1. Definisanje strateških i taktičkih ciljeva programa metrike;
2. Izbor metrike;
3. Razvoj strategije za primenu metrike;
4. Uspostavljanje referentnih performansi i ciljeva poboljšanja;
5. Određivanje načina prezentovanja metrike;
6. Definisanje akcionog plana i akcija za izvođenje programa metrike zaštite; i
7. Uspostavljanje formalnog ciklusa preispitivanja programa metrike.

Na ovaj način obezbeđuje se kontrolisan proces uspostavljanja programa metrike zaštite, konzistentnost sa njenim ciljevima i kako, ko i kada treba da koristi njene rezultate. Koraci uspostavljanja programa metrike zaštite ilustrovani su na Slika 3 i opisani u narednom tekstu.



Slika 3 Uspostavljanje programa metrike zaštite informacija

2.3.1 *Definisanje strateških i taktičkih ciljeva programa metrike*

Pošto razvoj i održavanje programa metrike zaštite zahteva angažovanje resursa iz svih procesa zaštite, kritičan faktor za optimizaciju truda i troškova je da se prvo dobro definišu ciljevi programa metrike. Iako ne postoji pravilo za jasno i brzo definisanje ciljeva programa metrike, dobar pristup je da rukovodstvo u formi izjave formuliše ciljeve na visokom, organizacionom, nivou, koji će sva merenja i metriku usmeravati u jednom pravcu. Na primer, izjava strateških ciljeva metrike zaštite može da glasi:

Obezbediti metriku koja jasno i jednostavno prezentuje efektivnost i efikasnost izbalansiranosti procenjenih bezbednosnih rizika i preventivnih mera zaštite, tako da se ulaganje u celokupan program zaštite može na najbolji način ograničiti i usmeriti ka uspostavljenim bezbednosnim ciljevima organizacije.

Izjave taktičkih ciljeva programa metrike treba da sadrže ključne aktivnosti i da se oslanjaju na prethodno uspostavljene strateške ciljeve, a akcioni plan mora biti direktno izveden iz tih izjava. Na primer, nekoliko taktičkih ciljeva koji proizilaze iz zahteva prethodne izjave su:

- a) *Bazirati program metrike na implementiranim praksama poboljšanja procesa u našoj kompaniji.*
- b) *Iskoristiti sva relevantna postojeća merenja performansi zaštite.*
- c) *Prezentovati metriku u formi koja odgovara zahtevima zainteresovanih strana.*
- d) *Uključiti relevantne učesnike u izbor metrike.*

2.3.2 Izbor metrike

Ako u preduzeću već postoji okvir za unapređenje procesa, metrike se prilagođavaju njemu. Na primer, “Six Sigma” je pristup koji usmerava procese zaštite na otkrivanje i upravljanje defektima, pa će u ovom koraku biti potrebno identifikovati specifične procese zaštite koji se odnose na defekte. Ako je pristup preduzeća zasnovan na usklađenosti, tada se metrika usmerava na ocenu stepena ispunjenja zahteva standarda. U ovom slučaju, treba identifikovati standarde koji nude odgovarajuću metriku. Na primer, standard ISO/IEC 27004, nudi metriku za sertifikacioni standard upravljanja zaštitom informacija ISO/IEC 27001. Ako ne postoji ovakav upravljački okvir procesa zaštite, za određivanje odgovarajuće metrike se koristi pristup odozgo na dole ili odozdo na gore. U Tabela 4 dat je pristup odozgo na dole, koji počinje sa ciljevima programa zaštite, preko identifikovanja specifičnih metrika za određivanje zadovoljenja tih ciljeva i završava sa merenjima potrebnim za izradu metrike.

Tabela 4 Pristup za izbor metrike – Odozgo na dole

PRISTUP ODOZGO NA DOLE		
a. Navesti ciljeve celokupnog programa zaštite	Primer ciljeva:	Do kraja sledeće godine redukovati broj virusnih infekcija za 30%.
b. Identifikovanje metrike koja bi mogla da prati progres svih ciljeva	Primer metrike:	Broj antivirusnih alarma u odnosu na presek stanja od pre dve godine.
c. Odabrati merenja potrebna za svaku metriku	Primeri merenja:	Broj antivirusnih alarma po mesecu. Broj prijavljenih infekcija.

U Tabela 5 dat je pristup odozdo na gore, gde provo treba da se ustanovi koji su procesi zaštite, proizvodi, servisi i sl. već izmereni, ili ih treba meriti, potom treba razmotriti koju metriku je moguće izvesti iz tih merenja i na kraju odrediti veze metrika sa ciljevima celokupnog programa zaštite.

Tabela 5 Pristup za izbor metrike – Odozdo na gore

PRISTUP ODOZDO NA GORE		
a. Identifikovati merenja koja su, ili bi mogla biti, prikupljena za taj proces zaštite	Primer merenja:	Prosečan broj detektovanih ranjivosti prvog stepena na svakom serveru po odeljenjima, korišćenjem alata za skeniranje ranjivosti
b. Određivanje metrike koja bi se mogla izraditi na osnovu odabranih merenja	Primer metrike:	Promena broja kritičnih ranjivosti detektovanih na serverima odeljenja u periodu od poslednjeg izveštaja o ranjivostima
c. Određivanje veze između izvedenih metrika i uspostavljenih ciljeva programa zaštite	Cilj:	Redukovati nivo detektovanih ranjivosti na serverima svih odeljenja preduzeća

Pristup odozgo na dole je mnogo bolji za identifikovanje metrika koje će biti usaglašene sa ciljevima celokupnog programa zaštite, dok je se pristup odozdo na gore lakši za određivanje metrike. Oba pristupa kreću od pretpostavke da su ciljevi celokupnog programa zaštite već uspostavljeni, jer su oni preduslov za izradu programa metrike zaštite informacija u organizacijama koje nemaju uspostavljen okvir za upravljanje procesima zaštite.

Svi korisnici metrika zaštite ističu značaj definisanja namene metrike, podataka koje treba prikupiti i načina prezentovanja rezultata zainteresovanim stranama. Zato, pre svih narednih akcija treba definisati i razumeti zahteve svih zainteresovanih strana. Zahtevi će

obezbediti razloge za angažovanja na izradi metrike zaštite. Metrika zaštite informacija organizaciji pomaže da se:

- a) Upravlja zaštitom informacija i integriše sa poslovanjem;
- b) Ispuni, održava i demonstrira usklađenost sa regulativama, zakonima, standardima i politikama zaštite;
- c) Meri i unapređuje efektivnost i efikasnost mehanizama i kontrola zaštite informacija;
- d) Opravda i predstavi značaj, vrednost i doprinos zaštite informacija za organizaciju;
- e) Identifikuj i redukuju rizici;
- f) Obezbede kvantitativne i objektivne mere performansi; i
- g) Predstave rezultati metrike netehničkom rukovodstvu i osoblju.

Ukoliko odabrana metrika zaštite ne ispunjava neke od navedenih zahteva, onda treba odabrati alternativnu metriku zaštite. U praksi je redak slučaj da jedna metrika zaštite može da ispuni sve zahteve.

Pre prikupljanja podataka treba razumeti zahteve i imati jasne ciljeve, a ne uzaludno trošiti vreme na prikupljanje beskorisnih informacija.

Definisanje i razumevanje zahteva zainteresovanih strana

Zainteresovane strane u organizaciji koje unapred imaju zahteve za metrikama zaštite su:

- Kolegijum direktora i izvršni direktori;
- IT menadžment i osoblje;
- Interni i eksterni auditori;
- Menadžment i osoblje za zaštitu informacija.

Najčešći zahtevi pomenutih zainteresovanih strana navedeni su u Tabela 6.

Tabela 6 Najčešće potrebe pojedinih zainteresovanih strana

	Kolegijum direktora	Izvršni direktori	Rukovodilac sistema zaštite informacija	Auditori	Rukovodilac IT zaštite
Veza sa tržištem	√	√	√	√	√
Identifikovanje i upravljanje rizikom	√		√	√	√
Merenje performansi	√	√	√	√	
Potvrda usklađenosti	√	√		√	√
Merenje kontrola		√	√	√	
Značaj zaštite informacija	√	√	√		
Upravljanje zaštitom informacija			√		√

Za svaku zainteresovanu stranu potrebno je izraditi specifičnu metriku zaštite.

Identifikovanje ulaza sa rukovodstvom i osobljem

O podacima koji će se koristiti u metrikama treba prodiskutovati sa poslovođstvom, menadžerima i osobljem zaštite IT i informacija. Dogovorom se utvrđuje način da se podaci jednom prikupe i koriste više puta, čime se štedi vreme i trud koji bi se potrošio za prikupljanje nerelavntnih podataka. Takođe, diskusije pomažu da se metrika zaštite predstavi na pravi i razumljiv način svim zainteresovanim stranama. Ukoliko je moguće,

diskusiju treba voditi prema utvrđenom dnevnom redu (modelu ili nekoj formi prezentacije).

Kada se zaštita izražava novcu, posloводство je uvek zainteresovano.

Obezbeđenje finansijskih sredstava

Korišćenje metrike zaštite, prikupljanje podataka za metriku, analiza i prezentacija uvek imaju uticaja na finansije. Nabavka ili razvoj softvera koji će automatizovati aktivnosti koje se odnose na metriku zaštite, najverovatnije će uvećati fondove za program metrike zaštite.

Fondove za metriku zaštite treba obezbediti u procesu planiranja novog budžeta, ili korišćenjem novca iz postojećeg. Kada se implementiraju metriku zaštite, osim za tekuću godinu, treba obezbediti fondove i za naredne godine, na primer, za razvoj i unapređenje metrike zaštite i metoda prezentovanja.

Kompanije u Velikoj Britaniji godišnje ukupno potroše oko pola miliona funti na unapređenje svojih programa metrika zaštite informacija.

Najčešće korišćene metriku zaštite informacija

Na osnovu anketa korisnika metrika zaštite, diskusija sa konferencija i istraživanja na internetu, identifikovane su najčešće korišćene metriku zaštite informacija i tipovi ulaznih podataka, [8]. U Tabela 7 navedene su metriku zaštite i primeri prikupljenih podataka, koji su uglavnom prikupljeni manuelno, nekonzistentno i sporo.

Tabela 7 Najčešće korišćene metriku zaštite informacija

Metrika zaštite	Primeri prikupljenih podataka
Incidenti	• broj incidenata u određenom periodu • uporedni prikaz broja incidenata u određenom periodu sa brojem incidenata u prethodnim periodima • broj glavnih ili poslovno-kritičnih incidenata • troškovi rešavanja određenog incidenta • broj identifikovanih ranjivosti • broj saniranih ranjivosti
Zaštita od virusa	• broj incidenata određenog tipa virusa • ukupan broj virusnih incidenata u određenom periodu • uporedni prikaz broja virusnih incidenata u određenom periodu sa brojem virusnih incidenata u prethodnim periodima • broj ažuriranja baze poznatih virusa • procenat uspešnih ažuriranja baza virusa • broj blokiranih virusa na gateway/perimeter
Upravljanje rizikom	• broj izvršenih analiza rizika • broj preispitivanja pretnji i ranjivosti • broj identifikovanih visokih/kritičnih bezbednosnih rizika • broj smanjenih visokih/kritičnih bezbednosnih rizika
Upravljanje pečevima	• broj evidentiranih/pečovanih ranjivosti (u određenom periodu) • merenje procesa (npr. izvršavanje koraka procesa u zadatom vremenu) • vreme utrošeno na pečovanje (npr. računarske imovine ili kritičnih sistema/aplikacija) • procenat pečovanja sistema u odnosu na Service Level Agreement ili politiku • procenat otkaza sistema koji nisu bili pečovani
Usaglašenost sa internim politikama	• broj izvršenih obuka za zaštitu informacija • broj povreda politika kompanije

Metrika zaštite	Primeri prikupljenih podataka
Nalazi <i>audit</i> -a	• broj neusaglašenosti otkrivenih internim auditom • broj neusaglašenosti otkrivenih eksternim auditom (npr. neusklađenost sa regulativama za zaštitu informacija li ugovornim obavezama) • srednje vreme rešavanja neusaglašenosti • procenat preostalih neusaglašenosti
Troškovi	• ukupni finansijski gubici (npr. pad prodaje, porudžbina ili proizvodnje) zbog narušavanja bezbednosti informacija • ukupni troškovi zbog povrede regulativa ili ugovornih obaveza • ukupni finansijski gubici zbog prevara, uključujući parnične troškove i troškove oporavka • ukupni troškovi zaštite (cena kontrola zaštite i posledica incidenata)

Primeri najčešće korišćenih metrika (Tabela 7), ne odgovaraju u potpunosti kategorijama (*broj, frekvencija, trajanje i cena*) i primerima datim u Tabela 3. Tabela 3 navodi par metrika koje se odnose na trajanje ili frekvenciju, a ostale na broj, cenu ili događaj. Kao rezultat, nije dobijena potpuna slika stanja bezbednosti, jer nisu prikupljeni svi bezbednosno relevantni podaci.

2.3.3 Razvoj strategije za primenu metrike

Pošto je sada jasno šta treba meriti, potrebno je razviti strategiju za prikupljanje mernih podataka i primenu metrike nad ovim podacima. Ove strategije treba da sadrže:

- izvore podataka,
- periodičnost prikupljanja,
- odgovornosti za tačnost prikupljenih sirovih podataka,
- način kombinovanja podataka za dobijanje mernih rezultata i
- izvođenje metrike.

Iako se u metrikama koriste podaci formalnog procesa procene rizika, stručnjaci su saglasni da njihove vrednosti ne treba koristiti. Postoje mišljenja da kvalitativna procena rizika daje približno tačnu metriku i da je takva procena rizika nestandardizovana i previše subjektivnog karaktera. Kao drugi izvori podataka mogu da se koriste zapisi reklamacija, sistemski logovi, firewall logovi, rezultati internih *audit*-a i anketa, itd.

Za prikupljanje podataka, analizu i generisanje izveštaja o isplativosti zaštite, mogu da se koriste automatizovani alati, koji su danas mnogo unapređeni i dostupni na tržištu.

Prikupljanje ulaznih podataka za metrike zaštite informacija

Podaci imaju različite oblike i mogu se prikupljati sa različitih lokacija. Veza između metrika zaštite i podataka ilustrovana je na Slika 4.



Slika 4 Veza između metrike zaštite i podataka

Prikupljanje podataka za metriku zaštite mora da bude konzistentno i precizno. Pre prikupljanja, treba biti siguran u tačnost ulaznih podataka koje će metrika koristiti, kao i u pouzdanost same metrike zaštite informacija.

Podaci, njihove lokacije i mehanizmi za prikupljanje moraju biti unapred definisani. Tipični primeri uključuju:

- ime odgovornog za prikupljanje podataka,
- namena prikupljenih podataka (u koju svrhu će se koristiti prikupljeni podaci),
- izvor podataka (logovi, izveštaji trećih strana,...),
- frekvencija prikupljanja (časovna, dnevna, nedeljna),
- metod prikupljanja (automatsko ili manuelno prikupljanje) i
- format podataka (numerički, tekstualni, ili kombinovani).

Pored bezbednosno orjentisanih podataka, treba prikupljati i kontekstualne podatke (npr. broj servera, osoblja i sl.). Upravljanje različitim aktivnostima prikupljanja biće olakšano ako se izradi plan prikupljanja podataka.

Podaci za metriku zaštite prikupljaju se:

- konzistentno i precizno,
- u skladu sa definisanim i usvojenim planom,
- prema imenovanim pojedincima od kojih se prikupljaju podaci i
- korišćenjem usvojenih šablona i formata (pisane forme ili unos podataka u baze).

Takođe, pre skladištenja podataka treba proveriti da li ima grešaka. Prilikom primene plana i preciznog prikupljanja podataka, treba voditi računa o zaštiti poverljivosti, kako ulaznih podataka, tako i same metrike zaštite.

Izvori podataka za metriku zaštite mogu biti interni (npr. statistika zaštite od virusa, izveštaji o incidentima i finansijski podaci) i eksterni (npr. broj ranjivosti operativnih sistema, broj izdatih pečeva proizvođača).

U procesima izbora metrike i razvoja strategije za njenu primenu, vrši se analiza i agregacija prethodno prikupljenih podataka, analiza same metrike i provera mogućnosti korelacije podataka:

1. Analiza i/ili agregacija prikupljenih podataka
 - Pre prezentovanja ili korišćenja metrika zaštite, treba izvršiti analizu prikupljenih podataka. Da bi se obezbedila uporedivost rezultata metrike, analiza ili agregacija podataka mora biti konzistentna.
 - Metodi analize mogu biti vremenske raspodele podataka (analize trendova ili predviđanja), jednostavne matematičke operacije (srednja vrednost, oduzimanje ili sabiranje), ili mnogo kompleksniji statistički računi. Takođe, podaci se mogu agregirati u viši nivo apstrakcije, bez detaljnih informacija.
2. Analiza metrike zaštite
 - Pored analize podataka, treba analizirati i unapređivati same metrike. Ovakve analize uključuju trendove ili predviđanja, upoređivanje sa referentnim metrikama, ranijim rezultatima i kontekstualnim podacima.
3. Provera korelacije podataka
 - U procesu analize podataka otvaraju se mogućnosti za identifikovanje korelacije između događaja, troškova i drugih kriterijuma.
 - Svaka identifikovana korelacija podataka mora pažljivo da se proveri, jer može lako da se desi da nije dobra.
 - Korelacijama se povezuju podaci koji često bolje predstavljaju zaštitu od pojedinačne ili agregirane metrike.

Prikupljanje kontekstualnih podataka

Kontekstualni podaci se koriste za poređenja, npr. “u samo 1% primljenih *e-mails* (1000 od 100000) otkriven je neprikladan sadržaj.” U ovom primeru, kontekstualni podatak je broj primljenih *e-mails*, a bezbednosna informacija je broj neprihvatljivih *e-mails*.

Izbor kontekstualnih podataka zavisi od namene metrike zaštite. U nekim slučajevima podatke je teško prikupiti ili identifikovati, što može dovesti do komplikacija, npr. nemogućnost postavljanja metrika zaštite u poslovni kontekst.

Kontekstualni podaci predstavljaju opštu sliku organizacije i na taj način omogućavaju da se zaštita informacija i metrike zaštite postave u odnos sa poslovanjem, što pomaže u da sve zainteresovane strane shvate namenu metrike.

Da bi bila razumljiva, metrika mora imati kontekst.

Normalizacija i skladištenje podataka

Podatke treba normalizovati (npr. duple zapise obrisati) i skladištiti ih u istom formatu. Skladištenje podataka treba da bude konzistentno, na primer, korišćenjem definisanih polja za sve tipove podataka i/ili metrika zaštite.

Karakteristike metrika zaštite mogu da se iskoriste za definisanje atributa u tabelama baza podataka, kao u primeru za definisanje kategorija zaštite (Tabela 3).

Treba imati jednu lokaciju za skladištenje (neki korisnici metrika sugerišu da se koriste namenski serveri za skladištenje podataka metrika zaštite informacija).

Dobro je imati zaštićen i namenski server za metriku zaštite, ali još bolje je imati tačne i pouzdane informacije.

2.3.4 Uspostavljanje referentnih performansi i ciljeva poboljšanja

U ovom koraku identifikuju se odgovarajuće referentne performanse (*benchmarks*) i zadaju ciljevi za unapređenje. Merenje performansi je proces upoređivanja sopstvenih performansi zaštite sa zvaničnim performansama najboljih industrijskih praksi. Ovaj proces stimuliše razvoj novih ideja za upravljanje aktivnostima programa, daje komparativne podatke za potvrdu primenjivosti metrike i pomaže u određivanju realnih ciljeva za poboljšanje postojećih praksi.

Menadžer zaštite mora aktivno da prati sve aktuelnosti industrijskih praksi koje mogu poslužiti kao reper performansi i praksi zaštite, kao i metrike publikovane od strane *SecurityStats.com*,⁸ *CIO Magazine*⁹ i ostalih servisa i korisnih publikacija.

2.3.5 Određivanje načina prezentovanja metrike

Sav trud uloženi u program metrike neće se isplatiti ako se rezultati ne prezentuju na efektivan način. Ipak, treba biti oprezan sa pojednostavljivanjem prezentacije, jer preterana pojednostavljenost može izazvati kontra efekat kod predstavnika finansijskog sektora i marketinga, kojima kompleksni podaci mogu biti od koristi. U svakom slučaju, grafička reprezentacija metrike je najefektivnija.

Neke metrike treba prezentovati samo menadžerima i osoblju zaštite informacija, dok menadžeri zaštite mogu koristiti i druge metrike kao dodatni element za upravljanje aktivnostima zaštite. Na primer, opšta metrika zaštite (za sve zainteresovane strane), kao

⁸ <http://www.securitystats.com>

⁹ <http://www.cio.com>

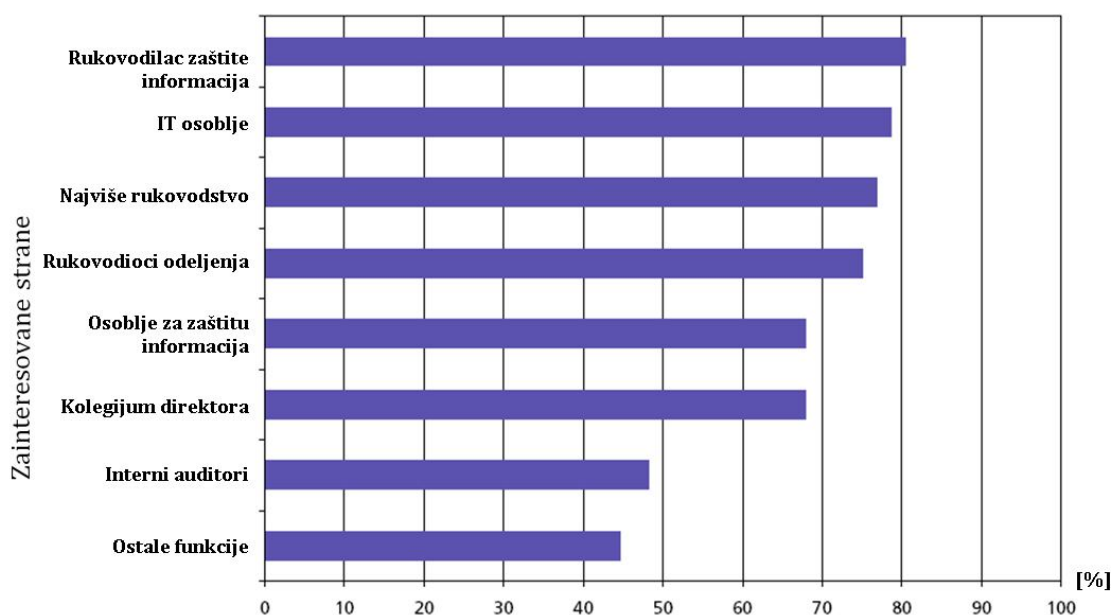
što je prikazivanje nivoa ranjivosti po organizacionim celinama preduzeća, može pokrenuti korisno takmičenje među odeljenjima, da u sledećem izveštaju imaju manje ranjivosti od ostalih odeljenja (ovo je san svakog menadžera zaštite).

U svakom slučaju, kontekst, forma, periodičnost, metod i odgovornost za distribuciju izveštaja metrike treba definisati na početku, tako da krajnji rezultat vizuelno odgovara onima koji generišu metriku i onima koji će koristiti njene rezultate za donošenje odluka.

Najčešće forme prezentovanja metrika zaštite informacija

Metrike zaštite obično se prezentuju kolegijumu direktora, rukovodiocu zaštite informacija i IT osoblju. Koriste se različite metode prezentovanja, a najčešći su dijagrami, instrument table i izveštaji, [8].

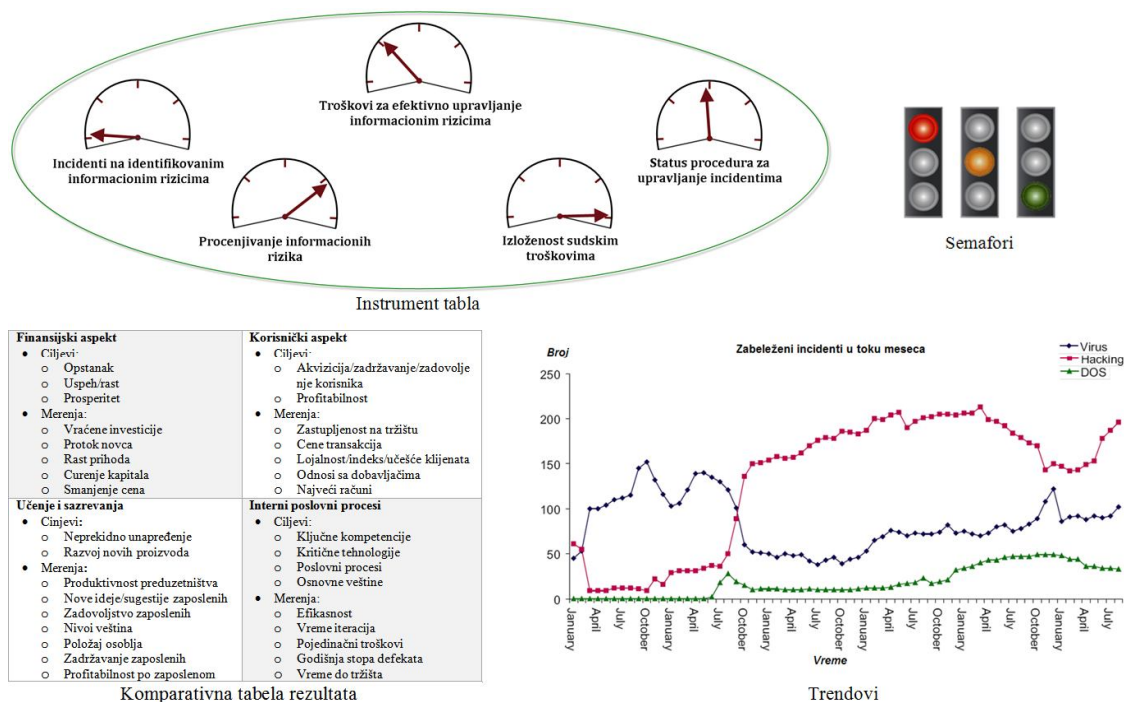
Na Slika 5 ilustrovan je uporedni prikaz zainteresovanih strana za metriku zaštite informacija. U predstavljanju rezultata metrike korišćeni su različiti načini prezentovanja, uključujući tabele, grafikone, komparativne tabele rezultata, semafore i instrument table (Slika 6).



Slika 5 Uloge u organizaciji kojima se najčešće prezentuju metrike zaštite

Kod više od tri četvrtine ispitanika, metrike zaštite prezentovane su rukovodiocima zaštite informacija i IT osoblju, a više od dve trećine kolegijumu direktora, ili sličnom telu u organizaciji.

Prezentovanjem metrika zaštite kolegijumu direktora obezbeđuje se dodatna podrška projektima zaštite informacija.



Slika 6 Primeri metoda za prezentovanje metrike zaštite informacija

Metode prezentovanja metrike uglavnom su grafičke, sa kvantitativnim ulazima i namerom da prenesu veliku količinu informacija na jasan i sažet način.

Dobro je imati instrument tablu, ali šta posle?

Instrument tabla je najpopularniji metod za prezentovanje rezultata kolegijumu direktora ili izvršnim direktorima, jer brzo i sažeto prikazuje veliku količinu podataka (0).

Zbog celovitosti i nepristrasnosti, grafikoni, semafori i tabele najčešće se prezentuju menadžerima zaštite ili IT osoblju. Grafikoni se često koriste za prezentovanje trendova i predviđanja.

Većina korisnika metrike tvrdi da korišćenje samo jedne metode prezentovanja ne deluje jednako na sve zainteresovane strane.

Prezentacija metrike zaštite treba da odgovara potrebama zainteresovanih strana i da bude razumljiva, jasna i sažeta. Način prezentovanja metrike određuje se prema zainteresovanim stranama, a njena efektivnost zavisi od pažljivog izbora metrike i stilova prezentacije.

Usklađivanje prezentacije prema zainteresovanim stranama

Format, stil, boje i kontekst prezentacije zavisi od zahteva zainteresovanih strana. Na primer, metrike koje se prezentuju predstavnicima zaštite informacija mogu da budu veoma detaljne, da uključuju log fajlove i tehničke probleme (crno-bele), dok za kolegijum direktora, prezentacija najčešće sadrži rezultate usklađenosti, uspehe na projektima i ključne poslovne rizike.

Bez obzira kome se prezentuje metrika zaštite, prezentacija mora biti razumljiva i efektivna. Da bi se prenela jasna i razumljiva poruka, potrebno je preispitati i testirati prezentaciju metrike zaštite, što će osigurati kvalitetnu interpretaciju rezultata metrike zaštite.

Ako se otkrije, razume i upotrebi forma i boje koje odgovaraju glavnom rukovodstvu, pažnja će biti usmerena na poruku, a ne na stil prezentacije.

Izbor načina prezentovanja

Najpopularnije forme prezentovanja metrike zaštite informacija su:

- Tabele sa sirovim podacima, analitičkim računima, ili statističkim podacima;
- Semafori, ili slični indikatori statusa;
- Instrument table;
- Komparativne tabele rezultata;
- Grafikoni za ilustrovanje trendova ili uporedno prikazivanje rezultata; i
- Izveštaji (npr. pisani tekst ili e-mail).

Tabela 8 može da posluži kao uputstvo za izbor metoda prezentacije, u odnosu na zainteresovane strane.

Tabela 8 Izbor načina prezentovanja metrike zainteresovanim stranama

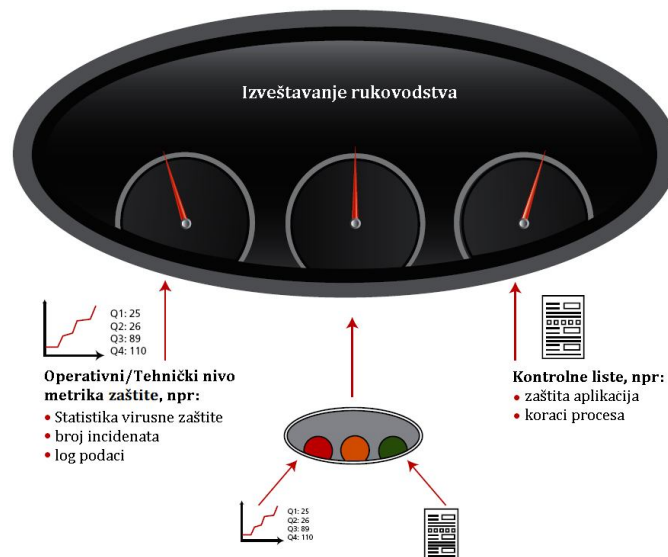
Način prezentovanja	Kolegijum direktora	Izvršni direktori	Rukovodilac sistema zaštite informacija	Auditori	Rukovodilac IT zaštite
Tabele			√	√	√
Semafori	√	√	√	√	√
Instrument table	√	√	√	√	√
Tabele rezultata	√	√	√		
Grafikoni/Trendovi		√	√		√
Izveštaji			√		√

Korišćenje jedne ili više formi prezentacija zavisi od zainteresovanih strana, poruke koja se želi preneti i zahtevanog nivoa detalja. Osnovna namena grafičkih metoda je da se prenese velika količina informacija na jednostavan i razumljiv način, koji nudi jasnu i komparativnu predstavu na visokom nivou apstrakcije. Ipak, treba uzeti u obzir činjenicu da izvršni direktori vrlo dobro razumeju detalje, zato uvek u rezervi treba imati i kompleksne grafikone.

Instrument table i tabele rezultata su dve najčešće i najkompleksnije metode prezentovanja metrike zaštite informacija. Obe metode mogu se koristiti za predstavljanje kompleksnih tehničkih podataka na najvišem nivou apstrakcije.

Instrument tabla

Instrument tabla je vizuelni metod prezentovanja performansi organizacije u odnosu na utvrđene kriterijume i može da se koristi zajedno sa ostalim grafičkim prezentacijama. Instrument tabla je veoma dobra komunikaciona alatka na najvišem nivou; dozvoljava agregaciju rezultata merenja performansi; može hijerarhijski prezentovati različite metrike zaštite, kako bi sve zainteresovane strane dobile odgovarajuće informacije. Primer instrument table ilustrovan je na Slika 7.



Slika 7 Primer korišćenja instrument tabli u metrikama zaštite informacija

Instrument tabla agregira detaljne podatke i trendove u jednostavnu ilustraciju. Da bi se predstavile performanse, detaljni ulazi (kontrolne liste, rezultati kontrole primene definisanih procesa, ili podaci logova) agregirani su i transformisani u brzinomer.

Prilikom korišćenja instrument table, pokreću se opšta pitanja koja podstiču odluke vezane za celokupan program zaštite informacija.

Komparativna tabela rezultata

Komparativna tabela rezultata je menadžerska alatka koja se podjednako koristi u upravljanju poslovanjem i upravljanju IT. Kada se tabela rezultata fokusira na operativni, korisnički, stručni i finansijski aspekt, tada obezbeđuje kompletnu sliku poslovanja. Primer poslovne komparativne tabele prikazan je u Tabela 9.

Tabela 9 Komparativna tabela rezultata

Finansijski aspekt	Korisnički aspekt
• Ciljevi: - o Opstanak - o Uspeh/rast - o Prosperitet • Merenja: - o Vraćene investicije - o Protok novca - o Rast prihoda - o Curenje kapitala - o Smanjenje troškova	• Ciljevi: - o Akvizicija/zadržavanje/zadovoljenje korisnika - o Profitabilnost • Merenja: - o Zastupljenost na tržištu - o Cene transakcija - o Lojalnost/indeks/učešće klijenata - o Odnosi sa dobavljačima - o Najveći računi

Učenje i sazrevanje • Ciljevi: - o Neprekidno unapređenje - o Razvoj novih proizvoda • Merenja: - o Produktivnost preduzetništva - o Nove ideje/sugestije zaposlenih - o Zadovoljstvo zaposlenih - o Nivoi veština - o Položaj osoblja - o Zadržavanje zaposlenih - o Profitabilnost po zaposlenom	Interni poslovni procesi • Ciljevi: - o Ključne kompetencije - o Kritične tehnologije - o Poslovni procesi - o Osnovne veštine • Merenja: - o Efikasnost - o Vreme iteracija - o Pojedinačni troškovi - o Godišnja stopa defekata - o Vreme do tržišta
---	---

Komparativna tabela rezultata uključuje samo generičke ciljeve i merenja u četiri različita aspekta. Većina korisnika metrika zaštite ističe brojne prednosti komparativne tabele rezultata, jer je prezentacija kompletna, sveobuhvatna i koristi formu koja odgovara poslovdstvu.

Komparativne tabele rezultata elegantno povezuju zaštitu informacija sa poslovanjem.

Mogućnosti za proširenje komparativne tabele rezultata

Koncept korišćenja komparativne tabele rezultata omogućava integrisanje standardnog okvira za upravljanje bezbednosnim rizicima (kontrola zaštite međunarodnog standarda ISO/IEC 27002) sa poslovnim zahtevima. Ovakve tabele su dobro prihvaćene među korisnicima metrika zaštite, čiji je dat u Tabela 10.

Tabela 10 Korišćenje tabele rezultata sa fokusom na standardne kontrole zaštite informacija

Finansijski aspekt 7. Upravljanje imovinom	Korisnički aspekt 5. Politika zaštite 6. Organizacija zaštite informacija 10. Upravljanje komunikacijama i operativnim radom 11. Kontrola pristupa 14. Upravljanje kontinuitetom poslovanja 15. Usklađenost
Učenje i sazrevanje 8. Bezbednost ljudskih resursa	Interni poslovni procesi 9. Fizička zaštita i zaštita radnog okruženja 13. Upravljanje bezbednosnim incidentom 12. Akvizicija, razvoj i održavanje informacionih sistema

Tabele rezultata sa fokusom na standardne kontrole zaštite informacija obezbeđuju opštu i kompletnu sliku svih bezbednosnih aktivnosti u organizaciji. Međutim, da bi korišćenje komparativnih tabela bilo efektivno, često treba predstaviti i dodatne informacije, uključujući finansijske podatke, detalje o incidentima i kontekstualnim podacima. Tada će jasno biti predstavljena kombinacija metrike zaštite sa ostalim informacijama specifičnim za organizaciju.

2.3.6 Definisane akcionog plana i akcija za izvođenje programa metrike zaštite

Sada je trenutak da se krene sa poslom. Akcioni plan treba da sadrži neophodne zadatke za pokretanje programa metrike, delegirane odgovornosti i datume izvršavanja akcija. Kao što je rečeno u koraku 2.3.1, akcije moraju direktno da se oslanjaju na uspostavljene

ciljeve programa metrike zaštite. Planiranje akcija obezbeđuje da svi učesnici imaju jasno dokumentovane zadatke.

2.3.7 Uspostavljanje formalnog ciklusa preispitivanja programa metrike

Formalno i periodično preispitivanje celokupnog programa metrike zaštite treba uspostaviti kao obavezan prateći deo celokupnog procesa izrade programa metrike zaštite. Takođe, u isto vreme treba voditi računa o nameni metrike zaštite i formi njene prezentacije zainteresovanim stranama. Rezultati preispitivanja metrike koriste se kao povratni mehanizmi za identifikovanje poboljšanja forme prezentacije.

Preispitivanje namene metrike zaštite

Rezultati preispitivanja metrike treba da obezbede kompletnost i balans u prezentaciji zaštite informacija preduzeća; da namena metrike bude razumljiva zainteresovanim stranama i da im obezbedi relevantne informacije za donošenje odluka.

U procesu preispitivanja mogu da se koriste pitanja, kao što su:

- Da li postoji sumnja u tačnost neke metrike?
- Da li su metrike korisne za usmeravanje novih akcija celokupnog programa zaštite?
- Koliko truda zahteva izrada metrike?

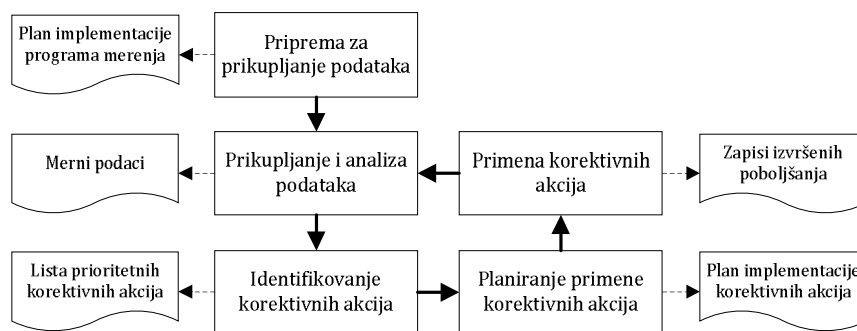
Za identifikovanje novih mogućnosti i rešenja koja mogu poboljšati program metrike treba pratiti nove standarde i najbolje prakse primene metrike zaštite informacija.

Preispitivanje prezentacione forme

Preispitivanje metrike treba da uključi i preispitivanje prezentacione forme, koja mora biti sažeta, prihvatljiva i razumljiva zainteresovanim stranama. Testiranje prezentacione forme je preporučljivo i obično se vrši na probnom sastanku sa predstavnicima zainteresovanih strana, gde se razmatraju predlozi i sugestije.

2.4 Implementacija programa merenja zaštite informacija

Slika 8 ilustruje pet faza procesa implementacije programa merenja zaštite informacija, koje, kad se u potpunosti izvrše obezbeđuju korišćenje merenja za kontinualno praćenje i poboljšanje performansi kontrola zaštite informacija, [5].



Slika 8 Proces implementacije programa merenja zaštite informacija

Merenje zaštite informacija vrši se u cilju, [9]:

- Evaluiranja efektivnosti implementiranih kontrola ili grupa kontrola;
- Verifikovanja stepena ispunjenja bezbednosnih zahteva;

- Doprinosa unapređenju performansi zaštite informacija u pogledu celokupnih poslovnih rizika organizacije; i
- Obezbeđenja ulaza u proces preispitivanja od strane rukovodstva, kako bi se doprinelo lakšem donošenju odluka koje se odnose na procese zaštite i opravdala potreba za njihovim unapređenjem.

Ciljevi merenja se određuju na osnovu brojnih faktora, od kojih su glavni sledeći:

- Uloga zaštite informacija u podršci poslovnih aktivnosti organizacije i kontroli bezbednosnih rizika;
- Zakonske i ugovorne obaveze za zaštitu informacija;
- Struktura organizacije;
- Troškovi i dobit od implementacije programa merenja zaštite informacija;
- Kriterijumi za prihvatanje bezbednosnih rizika; i
- Potreba za upoređivanjem sa ostalim sistemima zaštite informacija.

Organizacija treba da usvoji i implementira konstrukciju merenja koja će dati ponovljive, objektivne i korisne rezultate zasnovane na modelu merenja zaštite informacija (2.6).

Program merenja zaštite informacija i izgrađena konstrukcija merenja mora da osigura efektivno ispunjenje ciljeva i ponovljiva merenja i da obezbedi merne rezultate relevantne za zainteresovane strane, kako bi identifikovali potrebu za unapređenjem procesa zaštite, uključujući područje primene, politike, ciljeve, kontrole, procese i procedure zaštite.

2.4.1 Priprema za prikupljanje podataka

Prva faza procesa implementacije programa merenja zaštite informacija podrazumeva ključne aktivnosti za uspostavljanje osnovnog programa merenja zaštite informacija, uključujući identifikaciju, definiciju, razvoj i izbor merenja zaštite informacija. Sledeći korak je razvoj plana implementacije programa merenja zaštite informacija.

Koraci implementacije se definišu na prema načinu na koji će se podaci prikupljati, analizirati i prezentovati. Ove korake treba dokumentovati u planu implementacije programa merenja, koji uključuje:

- Zainteresovane strane;
- Uloge i odgovornosti za merenje, uključujući odgovornosti za prikupljanje podataka, analizu i izveštavanje;
- Proces prikupljanja, analize i prezentovanja merenja, usklađen sa specifičnom strukturom, procesima, politikama i procedurama organizacije;
- Koordinaciju aktivnosti odeljenja za bezbednost;
- Alate za praćenje, kreiranje ili selekciju kolekcije podataka;
- Alate za praćenje i modifikaciju kolekcije podataka; i
- Forme prezentacija merenja.

Pored toga, plan implementacije merenja uključuje rezultate aktivnosti monitoringa programa zaštite informacija. Rezultati kontinualnog monitoringa pružaju informacije koje u trećoj fazi doprinose prioritizaciji korektivnih akcija.

2.4.2 Prikupljanje i analiza podataka

Druga faza procesa implementacije programa merenja zaštite informacija osigurava da se prikupljeni podaci iskoriste za unapređenje zaštite informacionog sistema i identifikuju korektivne akcije. Aktivnosti ove faze uključuju:

- Prikupljanje podataka koji odgovaraju procesima definisanim u planu implementacije programa merenja;

- Agregaciju podataka radi dobijanja mera visokog nivoa apstrakcije (npr. podizanje merenja sa nivoa informacionog sistema na nivo merenja programa);
- Konsolidovanje prikupljenih podataka i skladištenje u formatu pogodnom za analizu i prezentovanje, na primer, u bazama podataka ili tabelama;
- Analizu propusta radi poređenja sa željenim performansama;
- Identifikovanje uzroka loših performansi; i
- Identifikovanje oblasti koje zahtevaju poboljšanja.

Nakon prikupljanja i kombinovanja dokaza, korektivne akcije se usmeravaju na otklanjanje uzroka problema (neefektivnosti, loših performansi ili neusaglašenosti sa zahtevima). Na primer, ako se pokaže da je procenat neodobrenih planova zaštite sistema na neprihvatljivom nivou, to neće biti od pomoći za otklanjanje problema. Potrebno je naći uzrok problema, kao što je nedostatak uputstava, stručnosti ili konflikt prioriteta. Primeri faktora koji doprinose neefektivnosti i lošoj implementaciji zaštite su sledeći:

- Resursi – Nedostatak ljudstva ili sredstava;
- Obuka – Nedostatak odgovarajuće obuke osoblja, administracije, održavanja ili primene informacionih tehnologija;
- Nadogradnje informacionog sistema – Bezbednosne popravke (*security patch*) koje nisu implementirane za vreme nadogradnje informacionog sistema;
- Prakse upravljanja konfiguracijom – Novi ili nadograđeni sistemi koji nisu konfigurisani prema bezbednosnim zahtevima;
- Kompatibilnost softvera – Bezbednosne popravke su nekompatibilne sa softverskim aplikacijama;
- Svest i posvećenost – Nedostatak svesti i/ili posvećenosti rukovodstva zaštititi informacija;
- Politike i procedure – Nedostatak politika i procedura neophodnih za funkcionisanje sistema zaštite informacija;
- Arhitektura – Loše arhitekture informacionog sistema i zaštite informacija koje informacione sisteme čine ranjivim; i
- Neefikasni procesi – Neefikasno planiranje i implementacija procesa otežava proces merenja.

2.4.3 Identifikovanje korektivnih akcija

Treća faza procesa implementacije programa merenja zaštite informacija, *Identifikovanje korektivnih akcija*, uključuje izradu plana koji će usmeravati aktivnosti rešavanja propusta implementacije identifikovanih u drugoj fazi. Treća faza uključuje sledeće aktivnosti:

- Određivanje obima korektivnih akcija – Na osnovu dobijenih faktora uzroka, identifikuju se potencijalne korektivne akcije svakog uzroka problema. Ove akcije mogu biti:
 - izmena konfiguracije informacionog sistema;
 - obuka osoblja za zaštitu informacija, osoblja za administraciju informacionog sistema, ili običnih korisnika;
 - naručivanje alata za zaštitu informacija;
 - promena arhitekture informacionog sistema;
 - uspostavljanje novih procesa i procedura; i
 - ažuriranje politika zaštite informacija.
- Prioritetizacija korektivnih akcija prema strateškim ciljevima za smanjenje rizika – Prioritetizacija sprovođenja korektivnih akcija vrši se prema troškovima ili uticaju problema performansi zaštite informacija na bezbednost, [6]; i

- Izbor najprikladnijih korektivnih akcija – Sa vrha liste najprioritetnijih korektivnih akcija biraju se one koje su najkritičnije i/ili najjeftinije.

2.4.4 Planiranje primene korektivnih akcija

Ova faza procesa implementacije programa merenja podrazumeva finansijsko planiranje za obezbeđenje resursa neophodnih za preduzimanje akcija ublažavanja uzroka problema identifikovanih u trećoj fazi, što uključuje sledeće:

- Dokumentovana misija i strateški ciljevi (identifikovani u drugoj fazi procesa razvoja merenja);
- Određivanje troškova i rizika održavanja nepromenjenog statusa koji će se koristiti kao referenca za alternativne investicije;
- Dokumentovani propusti performansi zaštite informacija identifikovani u drugoj fazi programa merenja zaštite informacija;
- Procena troškova životnog ciklusa svake korektivne akcije ili alternativnih investicija;
- Analiza osetljivosti, kako bi se odredilo koje ranjivosti imaju najveći efekat na troškove;¹⁰
- Karakterizacija dobiti (kvantitativna ili kvalitativna) od poboljšanih performansi, na osnovu prioritizacije korektivnih akcija utvrđene u trećoj fazi procesa implementacije programa merenja zaštite informacija;
- Analiza rizika kako bi se procenila verovatnoća otežavajućih okolnosti i rizici od primene određene alternative; i
- Priprema precizno opravdanog finansijskog plana, uzimajući u obzir ključne aspekte poslovanja, [13].

2.4.5 Primena korektivnih akcija

Peta faza procesa implementacije programa merenja zaštite informacija uključuje implementaciju korektivnih akcija u program zaštite, ili u tehničke, upravljačke ili operativne oblasti kontrole zaštite.

Iterativno prikupljanje, analiza i izveštavanje podataka će pratiti progres implementacije korektivnih akcija, unapređenja merenja i identifikovanja oblasti koja će kasnije zahtevati unapređenje. Priroda ciklusa prati napredak i osigurava da korektivne akcije utiču na implementaciju kontrole zaštite informacija na željeni način. Česta merenja performansi otkriće korektivne akcije koje nisu implementirane kako je planirano ili nemaju željeni efekat, što omogućava brze korekcije u organizaciji i eliminiše probleme koji se mogu otkriti u toku eksternih *audit*-a ili sličnih aktivnosti.

2.5 Obrasci za primenu merenja performansi zaštite informacija

Da bi se obezbedila ponovljivost aktivnosti razvoja, izrade, prikupljanja i izveštavanja, potrebno je imati dokumentovane rezultate merenja performansi. Standardnim formatom će se dati detaljan uvid u aktivnosti prikupljanja, analize i izveštavanja. Preporuke za izradu ovakvih obrazaca dati su u Tabela 11, [5] i Tabela 12, [10], a generička konstrukcija merenja zaštite informacija, sa elementima modela merenja performansi zaštite informacija (Slika 9), data je u Tabela 13, [9]. Pored ovih preporučenih obrazaca merenja, u zavisnosti od internih praksi i procedura, preduzeća mogu izraditi sopstvene obrasce za

¹⁰ Ako mala promena vrednosti promenjive uzrokuje veliku promenu u rezultatu, kaže se da je rezultat osetljiv na taj parametar ili je u pitanju pretpostavka.

merenje performansi i prilagoditi ih informacionim potrebama, kombinovanjem ili dodavanjem polja prema svojim zahtevima.

Tabela 11 Obrazac merenja zaštite informacija (NIST)

ID Merenja	Predstavlja jedinstveni identifikator koji se koristiti za praćenje i sortiranje merenja.
Strateški cilj	Izjave strateških i/ili bezbednosnih ciljeva.
Merenje	Merni iskaz. Koriste se numerički iskazi koji počinju sa rečima <i>procenat, broj, frekvencija, srednja vrednost</i> , nivoi uticaja (<i>visok, srednji, ili nizak</i>) i slično.
....	Izjava da li se meri implemetacija, efektivnost/efikasnost ili uticaj.
Formula	Kalkulacija za dobijanje mernih rezultata. Ulazi u formulu za izračunavanje merenja su informacije iz liste dokaza primene zaštite.
Očekivani cilj	Prag zadovoljavajuće nominalne vrednosti merenja, poput kontrolne tačke ispunjenja ciljeva ili statističke mere. Očekivani cilj može da se izrazi u procentima, vremenu, novcu ili drugim primenjivim mernim jedinicama. Očekivani cilj može biti vezan za zahtevani vremenski rok završetka. Konačni i privremeni cilj se bira radi praćenja progressa ka zadatom cilju.
Dokaz implementacije	Dokaz implemetacije se koristi kao ulaz za izračunavanje merenja, potvrda o izvršenim aktivnostima i za identifikovanje mogućih uzroka nezadovoljavajućih rezultata merenja. • Kod manuelnog ili automatskog prikupljanja podataka, dokazi implementacije identifikuju pitanja i elemente podataka koji će obezbediti neophodne ulazne vrednosti za izračunavanje merenja, kvalifikovanje prihvatljivosti merenja i validaciju obezbeđenih informacija. • Za svako pitanje ili upit, dokazi implementacije, ukoliko je primenjivo, daju broj implementiranih kontrola zaštite. • Dokazi implementacije mogu da se koriste za kvalitativno određivanje nivoa uticaja.
Periodičnost	Definiše koliko se često podaci prikupljaju, analiziraju i izveštavaju. Određivanje periodičnosti prikupljanja podataka vrši se na osnovu stope promene određenih kontrola zaštite koje su procenjivane i/ili prema internim prioritetima i eksternim zahtevima za podnošenje izveštaja.
Odgovorne strane	Ukazuje na sledeće ključne zainteresovane strane: • Vlasnik informacija: Identifikuje organizacionu komponentu i pojedinca koji poseduje zahtevane delove informacija; • Sakupljač informacija: Identifikuje organizacionu komponentu i pojedinca odgovornog za prikupljanje podataka (kada je moguće, uloga prikupljača informacija treba biti razdvojena, ili da bude predstavnik različite organizacione jedinice od vlasnika informacija, što eliminiše sukob interesa i obezbeđuje razdvajanje odgovornosti. Manje organizacije moraju odrediti da li je razdvajanje ovih odgovornosti izvodljivo; i • Korisnik informacija: Identifikuje organizacioni deo i pojedinca koji prima podatke.
Izvor podataka	Lokacija gde se nalaze podaci koji će se koristiti za izračunavanje merenja. Ovde su uključene baze podataka, alati za praćenje, organizacija ili specifične uloge u organizaciji koje mogu pružiti zahtevane informacije.
Format prezentovanja	Način na koji će merenja biti saopštena (razne vrste grafikona).

Tabela 12 Obrazac merenja zaštite informacija (ISO27k forum)

Naziv merenja	Treba da ukaže na to da li se meri implementacija, efektivnost/efikasnost ili uticaj.
Primarni klijenti	Interne zainteresovane strane za rezultate merenja.
Izvori podataka	Zapisi (radne aktivnosti, incidenti, transakcioni logovi, prethodni trendovi, zakonske i ugovorne obaveze, izveštaji primedbi klijenata, rezultati proveru, zahtevi za promenama, rezultati testiranja,...), sistem upravljanja ljudskim resursima, logovi pristupa, itd.
Formula	Zbir, procenat, srednja vrednost, kvalitativna procena i njihove matematičke kombinacije
Periodičnost	Godišnja, polugodišnja, kvartalna, itd.
Obrazloženje merenja	Zbog čega vršimo ovo merenje i šta ćemo njime postići.

Relevantne kategorije zaštite standarda ISO/IEC 27002	4. Upravljanje rizikom 5. Politika zaštite 6. Organizacija zaštite informacija 7. Upravljanje imovinom 8. Bezbednost ljudskih resursa 9. Fizička zaštita i zaštita radnog okruženja 10. Upravljanje komunikacijama i operativnim radom	11. Kontrola pristupa 12. Akvizicija, razvoj i održavanje informacionih sistema 13. Upravljanje bezbednosnim incidentom 14. Upravljanje kontinuitetom poslovanja 15. Usklađenost <u>Označiti na koju kategoriju zaštite se primenjuje merenje</u>
Karakteristike merenja	Vodeće / Prateće / Povremeno Lako / Teško / Srednje Objektivno / Subjektivno / Razno Apsolutno / Relativno / Delimično Poverljivost / Integritet / Raspoloživost	<u>Označiti prirodu merenja</u>
Alternativno merenje	Definisati alternativni scenario merenja.	
Napomene	Navesti moguće uticaje, uzroke i predloge rešenja.	

Tabela 13 Generička konstrukcija merenja zaštite informacija (ISO/IEC)

Identifikacija konstrukcije merenja	
Naziv konstrukcije merenja	Naziv merenja
Numerički identifikator	Jedinstveni identifikator
Svrha konstrukcije merenja	Šta se postiže ovim merenjem (informacione potrebe).
Cilj procesa/kontrola	Cilj procesa i/ili kontrola zaštite informacija koji merimo.
Kontrola(1)/proces(1)	Proces i/ili kontrola zaštite informacija koji merimo.
Kontrola(2)/proces(2)	Opciono: budući procesi i/ili kontrole zaštite informacija (planirani ili implementirani) koji pripadaju isto mernoj grupi.
Objekat i atributi merenja	
Objekat merenja	Objekat (entitet) koji se karakteriše merenjem njegovih atributa. Objekti mogu biti procesi, planovi, projekti, resursi i sistemi ili komponente sistema.
Atribut	Osobina ili karakteristika objekta merenja, koja se može izraziti kvantitativno ili kvantitativno (manuelno ili automatizovanim sredstvima).
Specifikacija osnovne mere (za svaku osnovnu meru [1...n])	
Osnovna mera	Osnovna mera se definiše za svaki atribut i utvrđeni metod merenja za njeno kvantifikovanje (npr. broj obučenog osoblja, broj sajtova, ukupni troškovi do tog datuma,...). Kako se koji podatak prikupi, tako se osnovnoj meri dodeli vrednost.
Metod merenja	Logičan redosled operacija kvantifikovanja atributa prema utvrđenom merilu.
Tip metoda merenja	Zavisno od karaktera operacija za kvantifikovanje atributa razlikujemo dve vrste metoda: • Subjektivna: kvantifikacija na osnovu lične ocene. • Objektivna: kvantifikacija na osnovu matematičkih operacija.
Merilo	Uređen skup vrednosti ili kategorija prema kojima se mapiraju atributi osnovnih mera.
Tip merila	Zavisno od prirode odnosa između vrednosti i merila, opšte prihvaćeni tipovi su: Nominalni, Ordinalni, Interval i Odnos.
Jedinica mere	Određena veličina, definisana i usvojena konvencijom, sa kojom se ostale istorodne veličine mogu uporediti tako da se njihov odnos može brojčano izraziti.
Specifikacija izvedene mere	
Izvedena mera	Mera koja je izvedena funkcijom merenja dve ili više osnovnih mera.
Funkcija merenja	Algoritam ili matematička operacija koja kombinuje dve ili više osnovnih mera. Merilo i jedinica izvedene mere zavisi od merila i jedinica osnovnih mera isto kao iz načina kombinovanja funkcijom merenja.
Specifikacija indikatora	
Indikator	Mera koja daje procenu ili evaluaciju specificiranih atributa izvedenih iz analitičkog modela u odnosu na definisane informacione potrebe. indikatori su osnova za analizu i donošenje odluka.

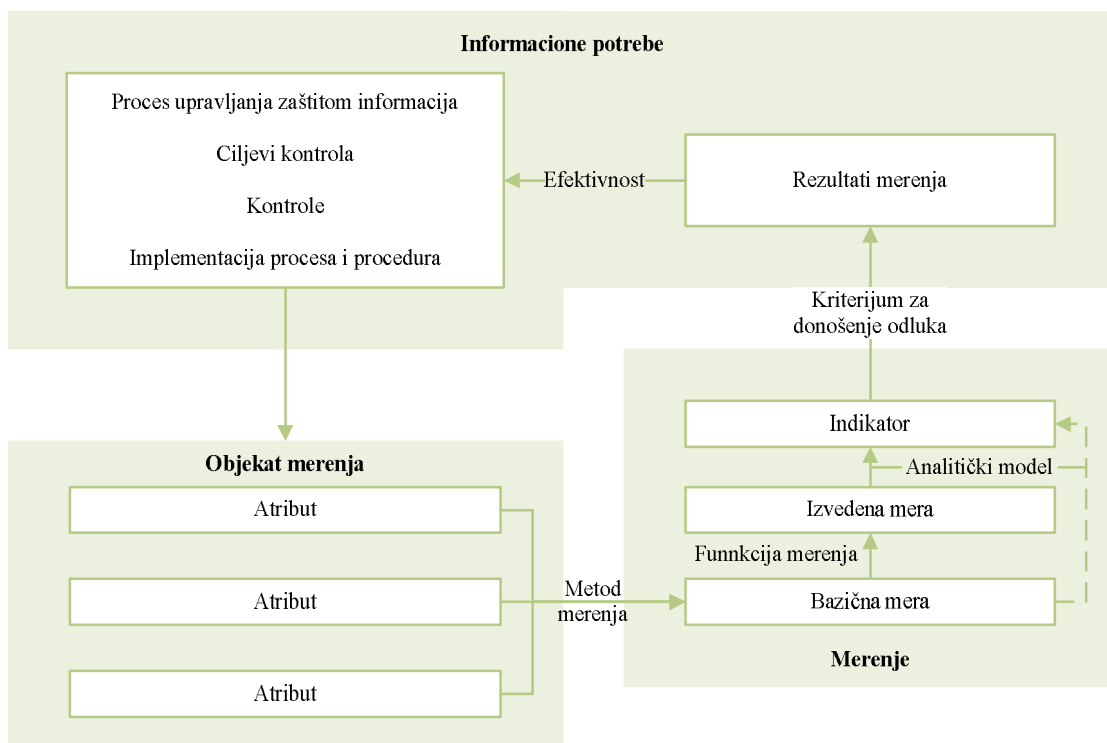
Analitički model	Algoritam ili kalkulacija koja kombinuje jednu i/ili više osnovnih mera u odnosu na uspostavljene kriterijume za donošenje odluka. Baziran je na razumevanju, ili pretpostavci, očekivane veze između bazične i/ili izvedene mere i/ili njihovim ponašanjem u toku vremena. Analitički model daje procene ili evaluacije relevantne za definisanje informacionih potreba.
Specifikacija kriterijuma za donošenje odluka	
Kriterijum za donošenje odluka	Prag, očekivani cilj, ili obrazac za određivanje potrebe za preduzimanjem akcija, istrage, ili opisivanjem nivo pouzdanosti predstavljenih rezultata. Kriterijum za donošenje odluka pomaže u interpretaciji rezultata merenja.
Rezultati merenja	
Interpretacija indikatora	Opis načina interpretacije indikatora (boje, senke, fontovi i drugi vizuelni načini isticanja).
Formati prezentovanja	Formati prezentovanja moraju biti identifikovani i dokumentovani. Ovde se definiše oblik prezentovanja koji odgovara potrebama organizacije ili vlasnicima informacija. Prezentaciona forma će vizuelno opisati merenja i otvoriti diskusiju o indikatorima performansi. Formatu prezentovanja moraju biti usklađeni prema korisnicima.
Zainteresovane strane	
Klijenti merenja	Rukovodstvo ili druge zainteresovane strane imaju potrebu ili zahtevaju informacije o efektivnosti sistema ili kontrola zaštite informacija.
Recinzent merenja	Osoba ili organizaciona jedinica koja validira da li je konstrukcija merenja prikladna za procenu efektivnosti sistema zaštite, kontrola ili grupa kontrola.
Vlasnik informacija	Osoba ili organizaciona jedinica koja poseduje informacije koje se odnose na objekat i atribut merenja i koja je ima odgovornosti za merenje.
Prikupljač informacija	Osoba ili organizaciona jedinica odgovorna za prikupljanje, zapisivanje i skladištenje podataka.
Komunikator	Osoba ili organizaciona jedinica odgovorna za analizu i saopštavanje podataka.
Periodičnost	
Periodičnost prikupljanja podataka	Koliko često se podaci prikupljaju.
Periodičnost analize podataka	Koliko često se vrši analiza podataka.
Periodičnost izveštavanja rezultata merenja	Kada se saopštavaju rezultati merenja (najčešće ređe od prikupljanja podataka)
Preispitivanje merenja	Datum preispitivanja merenja (nakon merenja ili istek ili obnova merenja)
Period merenja	U kom periodu se vrši merenje.

Ovakve forme merenja su dovoljne da u bilo kom trenutku odgovore zakonskim ili poslovnim obavezama izveštavanja stanja bezbednosti organizacije. Praktični primeri primene obrazaca merenja dati su u prilogima PRILOG A, PRILOG B i PRILOG C. Ovi primeri se mogu koristiti kao polazna osnova za merenje zaštite informacija, modifikovati prema specifičnim potrebama ili koristiti kao šabloni za sva ostala merenja zaštite informacija.

2.6 Model merenja performansi zaštite informacija

Model merenja zaštite informacija je struktura koja povezuje informacione potrebe sa relevantnim objektima merenja i njihovim atributima, [9]. Objekti merenja mogu biti planirani ili imlementirani procesi, procedure, projekti i resursi.

Model merenja zaštite informacija, ilustrovan na Slika 9, opisuje način kvantifikovanja i konvertovanja relevantnih atributa u indikatore performansi, koji će obezbediti osnovu za donošenje odluka.



Slika 9 Model merenja performansi zaštite informacija

2.6.1 Elementi modela merenja performansi zaštite informacija i primeri merenja

Informacione potrebe u Tabela 14 zahtevaju da se među relevantnim osobljem oceni razumevanje zahteva politike bezbednosti informacija (cilj kontrole A.8.2¹¹ i kontrole za ispunjenje cilja: A.8.2.1 i A.8.2.2, standarda ISO/IEC 27001:2005). Tabela 14 predstavlja primer primene modela merenja zaštite informacija za sledeće kontrole:

- “Kontrola 1” odnosi se na kontrolu *A.8.2.2 Bezbednosna svest, edukacija i obuka* (“Svi zaposleni i, gde je to relevantno, izvođači radova i eksterni korisnici moraju imati obuku i da redovno obnavljaju znanja o bezbednosnim politikama i procedurama, u skladu sa njihovim odgovornostima.”). Odavde je izvedena sledeća informaciona potreba: “Svo osoblje obuhvaćeno sistemom zaštite mora imati svest o potrebi zaštite informacija pre nego što im se dozvoli pristup informacionom sistemu.”
- “Kontrola 2” odnosi se na kontrolu *A.8.2.1 Odgovornost rukovodstva* (“Rukovodstvo od zaposlenih, izvođača radova i eksternih korisnika zahteva da primenjuju zaštitu prema uspostavljenim bezbednosnim politikama i procedurama organizacije.”). Odavde je izvedena sledeća informaciona potreba: “Svo osoblje relevantno za ISMS mora potpisati korisnički ugovor pre nego što im se dozvoli pristup informacionom sistemu.”

Kombinacije slova i brojeva u Tabela 14 označavaju da se sledeći element odnosi na prehodni, a strelice označavaju tok podataka među elementima (objekti merenja i njihovi

¹¹ Obezbediti da svi zaposleni, ugovorne i treće strane imaju: svest o pretnjama i svojoj ulozi u zaštiti informacija, odgovornosti i obaveze, opremu koja podržava politiku zaštite organizacije tokom njihovog normalnog rada, i smanjiti rizik ljudske greške.

atributi, metod merenja i osnovne mere za merenje objekata odabranih za gore opisane kontrole.

Osnovna mera i metod merenja

Osnovna mera se najlakše određuje. Ona predstavlja rezultat primene metoda merenja na attribute odabranih objekata merenja. Objekti (predmet) merenja mogu imati više atributa, od kojih samo neki od njih mogu biti korisni za određivanje osnovne mere. Jedan atribut može da se iskoriste za više osnovnih mera.

Metod merenja koristi logičke operacije za kvantifikovanje atributa objekata merenja u odnosu na utvrđena merila i metod merenja može primeniti attribute na objekat merenja. Neki od primera objekata merenja uključuju:

- Performanse implementiranih kontrola;
- Status informacione imovine zaštićene kontrolama;
- Performanse procesa zaštite;
- Ponašanje osoblja odgovornog za zaštitu;
- Aktivnost organizacionih jedinica odgovornih za zaštitu informacija; i
- Stepen zadovoljstva zainteresovanih strana.

Metodi merenja mogu koristiti objekte i attribute merenja iz različitih izvora, kao što su:

- Rezultati analize i procene rizika;
- Upitnici i intervjui;
- Izveštaji internih i/ili eksternih provera sistema zaštite;
- Zapisi događaja, kao što su logovi, statistički izveštaji i kontrolni tragovi;
- Izveštaji o incidentima;
- Rezultati testiranja, npr. testiranje proboja, socijalni inženjering, alati usklađenosti i alati provere bezbednosti; ili
- Zapisi procedura i programa zaštite informacija, npr. rezultati obuke razvoja svesti o potrebi zaštite informacija.

Izvedena mera i funkcija merenja

Izvedena mera je agregacija dve ili više osnovnih mera. Jedna osnovna mera može biti ulaz nekoliko izvedenih mera. Funkcija merenja je operacija nad više osnovnih mera za dobijanje izvedene mere, npr. srednja vrednost osnovnih mera ili dodela kvalitativnih vrednosti osnovnim merama. Ona kombinuje osnovne mere korišćenjem različitih veličina, kao što su procenat i rezultati kvalitativne ocene.

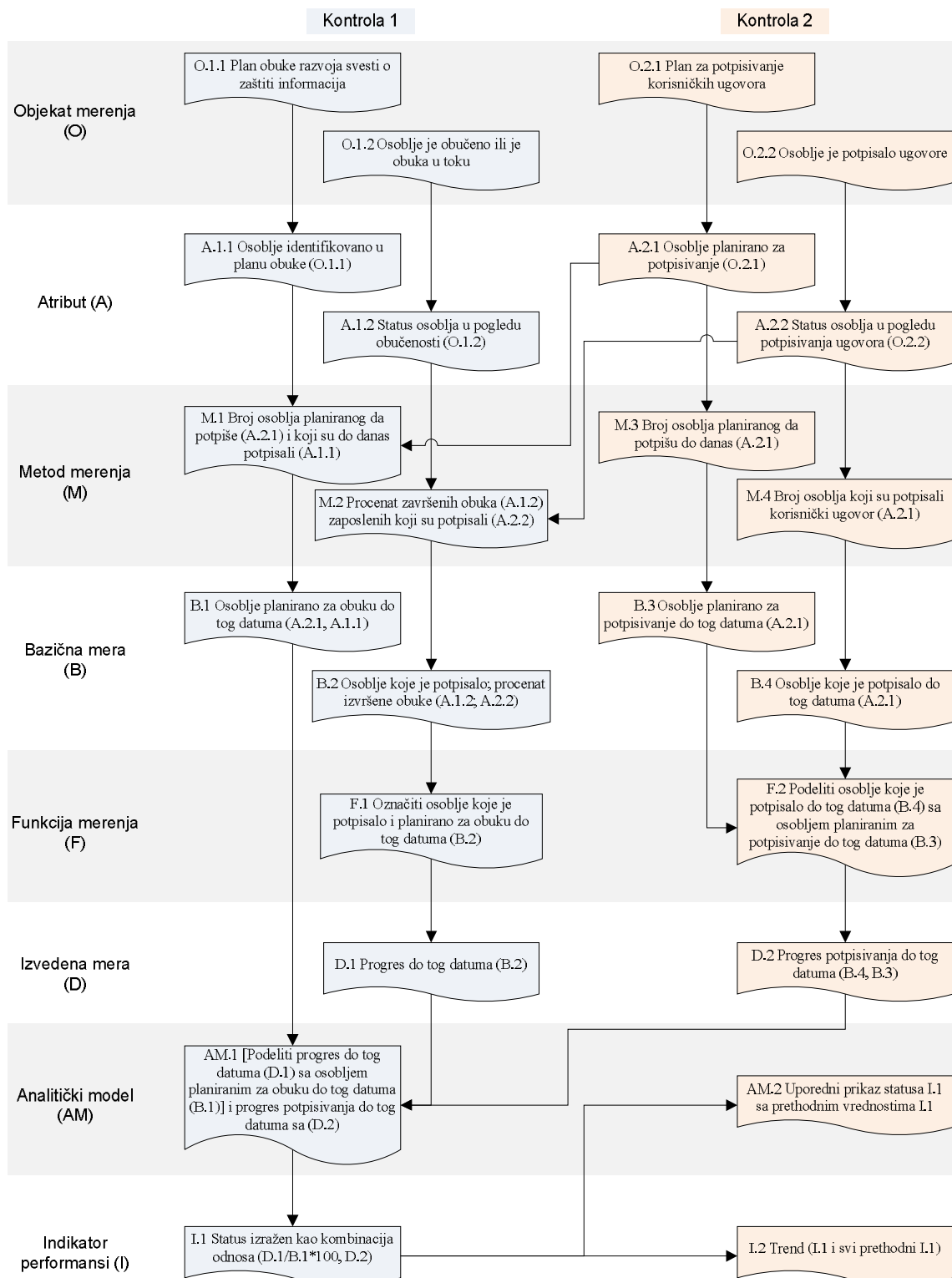
Indikatori performansi i analitički model

Indikator je mera koja omogućava procenu ili evaluaciju određenih atributa izvedenih analitičkim modelom prema definisanim informacionim potrebama. Indikatori se dobijaju primenom analitičkog modela na osnovne i/ili izvedene mere i njihovom kombinacijom sa kriterijumom za donošenje odluka. Na izbor analitičkih tehnika utiču merne jedinice i metod merenja. Često se zbog lakše prezentacije indikatori predstavljaju u grafičkoj formi.

Rezultati merenja i kriterijumi za donošenje odluka

Rezultati merenja su interpretacija odgovarajućih indikatora na osnovu definisanih kriterijuma i koriste se za ocenu efektivnosti sistema zaštite. Kriterijumi za donošenje odluka se koriste za utvrđivanje potrebe za preduzimanjem korektivnih/preventivnih akcija ili istragu, kao i za predstavljanje stepena poverenja u merne rezultate. Jedan kriterijum za donošenje odluka može da se primeni na niz indikatora, npr. za analizu trenda na osnovu indikatora dobijenih u različitim vremenskim periodima.

Tabela 14 Primer primene modela merenja za dobijanje indikatora performansi kontrola zaštite



2.6.2 Odgovornost rukovodstva u programu merenja zaštite informacija

Rukovodstvo je odgovorno za uspostavljanje programa merenja zaštite informacija, uključivanje zainteresovanih strana u aktivnosti merenja, preispitivanje rezultata merenja i njihovo korišćenje za unapređenje sistema zaštite. Da bi se ovo postiglo rukovodstvo treba da:

1. Upostavi ciljeve programa merenja zaštite informacija;
 - Očekivani ciljevi sadrže detaljne specifikacije performansi, primenjive na organizaciju ili njene delove, izvedeni su iz ciljeva zaštite informacija (poput ciljeva sistema ili kontrola zaštite informacija) i treba ih postaviti i ispuniti u pravcu zadovoljenja ovih strateških ciljeva.
2. Upostavi politiku programa merenja zaštite informacija;
 - Formalna obaveza za primenu merenja performansi zaštite informacija.
3. Obezbedi adekvatne resurse za merenje (osoblje, finansijska sredstva, alate i infrastrukturu);
 - Rukovodstvo mora da obezbedi resurse neophodne za ključne aktivnosti merenja zaštite informacija, kao što su prikupljanje podataka, analiza, skladištenje, izveštavanje i distribucija. Alokacija resursa uključuje:
 - resurse odgovorne za sve aspekte programa merenja zaštite informacija,
 - odgovarajuću finansijsku podršku i
 - odgovarajuću infrastrukturnu podršku, kao što su infrastruktura i alati za izvođenje procesa merenja.
4. Osigura da ciljevi programa merenja zaštite informacija budu ispunjeni;
5. Obezbedi pravilno održavanje alata i opreme za prikupljanje podataka;
6. Upostavlja svrhu merenja svake konstrukcije merenja;
7. Osigura da merenje obezbedi informacije neophodne za zainteresovane strane u pogledu efektivnosti i potreba za unapređenje sistema zaštite, uključujući područje primene, politike, ciljeve, kontrole, procese i procedure; i
8. Osigura da merenje obezbedi informacije za zainteresovane strane, u pogledu efektivnosti kontrola ili grupa kontrola i potreba za unapređenje kontrola zaštite.
 - Rukovodstvo treba obezbediti da zainteresovane strane:
 - dobiju adekvatnu obuku za svoje uloge i odgovornosti u programu merenja zaštite informacija i odgovarajuću kvalifikaciju za izvršavanje svojih uloga i odgovornosti i
 - razumeju svoje obaveze za donošenje preporuka za unapređenje programa merenja zaštite informacija.

Kako bi se izbegla pristrasnost vlasnika informacija¹², rukovodstvo mora da odredi uloge i odgovornosti za merenje i, gde je to moguće, da primeni princip razdvajanja dužnosti ili da se koristi detaljna dokumentacija merenja koja će omogućiti nezavisne provere programa merenja zaštite informacija.

2.7 Primena modela merenja performansi zaštite informacija

U ovom poglavlju opisan je način razvoja mera i merenja u cilju ocene efektivnosti sistema zaštite, kontrola ili grupa kontrola zaštite informacija i identifikovanje skupova

¹² Entitet ili osoba koja ima odgovornost, odobrenu od strane rukovodstva, za kontrolu, produkciju, održavanje, korišćenje i zaštitu imovine. Izraz 'vlasnik' ne podrazumeva da lice zaista ima vlasnička prava nad imovinom.

konstrukcija merenja koji su specifični za organizaciju. Proces merenja mora imati dokumentovane sledeće aktivnosti:

1. Definisane područja primene merenja
2. Identifikovanje informacionih potreba
3. Izbor objekata i atributa
4. Izrada konstrukcije merenja

Prilikom uspostavljanja ovih aktivnosti treba uzeti u obzir finansije, ljudstvo, infrastrukturu i alate.

2.7.1 Definisane područja primene merenja

Zavisno od kapaciteta i resursa inicijalno područje primene aktivnosti merenja biće ograničeno na specifične kontrole, informacionu imovinu zaštićenu tim kontrolama i najprioritetnije aktivnosti zaštite informacija. Područje primene kasnije može da se proširi na elemente koji sistema zaštite i kontrole ili grupe kontrola, uzimajući u obzir prioritete zainteresovanih strana.

U procesu definisanja područja primene aktivnosti merenja moraju učestvovati relevantne interne ili eksterne zainteresovane strane, npr. rukovodioci projekta, rukovodioci sistema zaštite informacija i donosioci odluka.

Rezultate merenja efektivnosti kontrola ili grupa kontrola treba definisati i saopštiti relevantnim zainteresovanim stranama. Donosiocima odluka treba predstaviti ograničen broj rezultata merenja i dati dovoljno vremena za primenu unapređenja sistema zaštite. Rezultate merenja treba postaviti prema prioritetima za unapređenje. Prioritetizacija rezultata merenja zaštite informacija mora da se bazira na značaju odnosnih informacionih potreba i ciljeva sistema zaštite.

2.7.2 Identifikovanje informacionih potreba

Svaka konstrukcija merenja mora biti formirana prema informacionim potrebama. Primeri informacionih potreba definišu se na početku procesa merenja kao svrha merenja i na kraju sa relevantnim kriterijumima za donošenje odluka (Tabela 13).

Za identifikovanje relevantnih informacionih potreba treba izvršiti sledeće aktivnosti:

- a) Ispitivanje sistema za upravljanje zaštitom informacija i njegovih procesa, kao što su:
 - 1) politika i ciljevi sistema, kontrola i kontrole zaštite informacija;
 - 2) zakoni, regulative i ugovorne obaveze zaštite informacija; i
 - 3) izlazi procesa upravljanja bezbednosnim rizicima.
- b) Prioritetizacija informacionih potreba na osnovu utvrđenih kriterijumima, poput:
 - 1) prioriteta treriranja rizika;
 - 2) kapaciteti i resursi organizacije;
 - 3) interesi zainteresovanih strana;
 - 4) politika zaštite informacija;
 - 5) informacije za ispunjenje zakonskih, regulativnih i ugovornih zahteva; i
 - 6) vrednost informacija u odnosu na cenu merenja zaštite informacija.
- c) Izbor podskupa informacija za merenje iz liste prioritetizacije; i
- d) Dokumentovanje i saopštavanje odabranih informacionih potreba relevantnim zainteresovanim stranama.

Sva relevantna merenja sistema, kontrola ili grupa kontrola zaštite informacija, moraju biti implementirana na osnovu odabranih informacionih potreba.

2.7.3 Izbor objekata i atributa merenja

Objekat merenja zaštite informacija i njegovi atributi moraju biti identifikovani u kontekstu i području primene sistema zaštite. Treba napomenuti da jedan objekat merenja može imati nekoliko primenjivih atributa. Objekat i njegovi atributi biraju se prema prioritetima informacionih potreba.

Primenom odgovarajućeg metoda merenja na odabrane attribute objekata merenja dobijaju se osnovne mere. Od karakteristika odabranih atributa zavisi koji tip metoda merenja treba koristiti za dobijanje vrednosti osnovnih mera (npr. kvalitativna ili kvantitativna). Primeri objekata merenja zaštite informacija mogu biti:

- Proizvodi i usluge;
- Procesi;
- Imovina (npr. osnovna sredstva, aplikacije i informacioni sistemi);
- Organizacione jedinice;
- Fizičke lokacije; i
- Usluge treće strane.

2.7.4 Izrada konstrukcije merenja

Izrada konstrukcije merenja podrazumeva sledeće aktivnosti:

1. Izbor merenja
2. Određivanje metoda merenja
3. Definisanje funkcije merenja
4. Izbor analitičkog model
5. Utvrđivanje indikator
6. Definisanje kriterijuma za donošenje odluka
7. Identifikovanje zainteresovanih stran

Izbor merenja

Izbor merenja podrazumeva određivanje tipa merenja koji će odgovarati informacionim potrebama i razmatranje kontekstualnih informacija za interpretaciju ili normalizaciju merenja. Odabrane mere moraju da odražavaju prioritet informacionih potreba. Kriterijumi za izbor merenja mogu biti:

- Lako prikupljanje podataka;
- Raspoloživost ljudskih resursa za prikupljanje i upravljanje podacima;
- Raspoloživost odgovarajućih alata;
- Broj potencijalnih relevantnih indikatora podržanih od strane osnovnih mera;
- Jednostavna interpretacija;
- Broj korisnika rezultata merenja; i
- Troškovi prikupljanja, upravljanja i analize podataka.

Određivanje metoda merenja

Metod merenja se definiše za svaku osnovnu meru i koristi se za kvantifikovanje objekata merenja transformacijom atributa u vrednosti koje se dodeljuju osnovnoj meri.

Postoje subjektivni (kvantitativni) i objektivni (kvalitativni) metodi merenja. Metod merenja kvantifikuje attribute u odnosu na utvrđeno merilo, koje je izraženo u odgovarajućim mernim jedinicama (direktno su uporedive samo one veličine koje su izražene u istim mernim jedinicama).

Za svaki metod merenja treba uspostaviti i dokumentovati proces verifikacije, kojim će se garantovati nivo poverenja u vrednosti bazičnih mera, koje se dobijene primenom metoda

merenja na attribute objekata merenja. Validne vrednosti osnovnih mera mogu da se dobiju standardizovanim alatima za dobijanje atributa. Takođe, treba uzeti u obzir preciznost metoda merenja i dokumentovati devijacije ili varijacije.

Definisanje funkcije merenja

Funkcija merenja se definiše za svaku pojedinačnu izvedenu meru, korišćenjem dve ili više vrednosti dodeljenih osnovnim merama. Ova funkcija merenja transformiše vrednosti jedne ili više osnovnih mera u vrednosti koje se dodeljuju izvedenim merama. U nekim slučajevima analitički model, pored izvedene mere, može direktno koristiti osnovnu meru.

Izbor analitičkog modela

Za svaki indikator definiše se analitički model koji transformiše jednu ili više vrednosti osnovnih i/ili izvedenih mera u vrednost koja se dodeljuje indikatoru. Analitički model kombinuje relevantne mere u cilju dobijanja rezultata bitnih zainteresovanim stranama.

Prilikom definisanja analitičkog modela uzima se u obzir kriterijum za donošenje odluka koji se primenjuje na indikator.

Utvrdjivanje indikatora merenja

Vrednosti indikatora se dobijaju agregacijom vrednosti izvedenih mera i interpretacijom tih vrednosti na osnovu kriterijumima za donošenje odluka.

Način prezentovanja indikatora takođe treba definisati. Format prezentovanja indikatora vizuelno opisuje merenja, pomažu u diskusiji i treba da budu prilagođeni informacionim potrebama klijenta.

Definisanje kriterijuma za donošenje odluka

Za svaki indikator se definiše i dokumentuje odgovarajući kriterijum za donošenje odluka, koji se zasniva na bezbednosnim ciljevima i pruža primenjive smernice zainteresovanim stranama. Ove smernice treba da ukažu na očekivanja od progresa i pragove za pokretanje akcija unapređenja zasnovanih na indikatorima.

Kriterijum za donošenje odluka uspostavlja očekivani cilj prema kome se meri uspeh i obezbeđuje uputstvo za interpretaciju indikatora u odnosu na njegovu blizinu ostvarenju tog cilja.

Očekivani ciljevi moraju biti postavljeni za svaki indikator performansi procesa i kontrola zaštite, ispunjenja ciljeva zaštite i efektivnosti sistema zaštite koja će biti evaluirana.

Rukovodstvo može odlučiti da ne zada očekivane ciljeve za idiktore dok se ne prikupe inicijalni podaci. Kriterijumi za donošenje odluka se definišu nakon identifikovanja korektivnih akcija na osnovu inicijalnih podataka. Nakon što se na osnovu inicijalnih podataka identifikuju korektivne akcije, definišu se odgovarajući kriterijumi za donošenje odluka i realne kontrolne tačke sistema zaštite. Ako se kriterijumi za donošenje odluka ne mogu uspostaviti na ovaj način, mora se preispitati da li će objekat merenja i odgovarajuće mere pružiti očekivane vrednosti za organizaciju.

Kriterijum za donošenje odluka može biti izveden iz istorijskih podataka, planova, pretpostavki, izračunatih kontrolnih granica ili statističkih granica poverenja. Prethodno posmatrani trendovi mogu dati uvid u nivoe prethodnih performansi i uputstvo za kreiranje realnog kriterijuma za donošenje odluka. Kriterijum za donošenje odluka može da se izračuna ili da se bazira na razumevanju koncepta očekivanog ponašanja.

Identifikovanje zainteresovanih strana

Za svaku osnovnu i/ili izvedenu meru treba identifikovati i dokumentovati odgovarajuće zainteresovane strane, kao na primer:

- klijenti merenja: rukovodstvo i druge zainteresovane strane zahtevaju informacije o efektivnosti sistema, kontrola ili grupa kontrola zaštite;
- recizent merenja: osoba ili organizaciona jedinica za validaciju da konstrukcija izrade merenja odgovara za procenu efektivnosti sistema, kontrola ili grupa kontrola zaštite;
- vlasnik informacija: osoba ili organizaciona jedinica koja poseduje informacije o objektu i atributima merenja i odgovorna za merenje;
- prikupljač informacija: osoba ili organizaciona jedinica odgovorna za prikupljanje, zapisivanje i skladištenje podataka; i
- komunikator: osoba ili organizaciona jedinica odgovorna za analiziranje podataka i saopštavanje rezultata merenja.

2.8 Evaluacija i unapređenje programa merenja zaštite informacija

Organizacija treba u planiranim intervalima da evaluiira sledeće, [9]:

- Efektivnost implementiranog programa merenja zaštite informacija, da bi se utvrdilo da program:
 - Daje efektivne rezultate merenja;
 - Prati plan programa;
 - Prikazuje promene u sistemu i kontrolama zaštite; i
 - Prikazuje promene u okruženju (npr. zahtevi, regulative, ili tehnologije).
- Korisnost rezultata merenja zaštite informacija da bi se utvrdilo da rezultati ispunjavaju relevantne informacione potrebe.

Rukovodstvo mora da odredi periodičnost ovih evaluacija, planira periodična preispitivanja i, ako je moguće, da uspostavi mehanizme za sprovođenje ovih preispitivanja, koje uključuju sledeće aktivnosti:

1. Identifikovanje kriterijuma evaluacije programa merenja zaštite informacija;
2. Nadzor, preispitivanje i evaluacija programa merenja zaštite informacija; i
3. Implementacija unapređenja.

2.8.1 Identifikovanje kriterijuma evaluacije programa merenja zaštite informacija

Organizacija mora da definiše kriterijume za evaluaciju efektivnosti programa merenja zaštite informacija i evaluaciju iskoristivosti dobijenih rezultata merenja. Kriterijumi moraju biti definisani na početku implementacije programa merenja zaštite informacija, uzimajući u obzir kontekst tehničkih i poslovnih ciljeva organizacije.

Najčešći kriterijumi koji se biraju kada organizacija želi da evaluiira i unapredi implementirani program merenja zaštite informacija su:

- Promene u poslovnim ciljevima organizacije;
- Promene u zakonskim i ugovornim obavezama za zaštitu informacija;
- Promene u bezbednosnim rizicima organizacije;
- Povećana raspoloživost mnogo prečišćenijih ili odgovarajućih podataka i/ili metoda za prikupljanje podataka za svrhe merenja; i
- Promene na objektima merenja i/ili atributima.

Za evaluaciju dobijenih rezultata merenja mogu da se primene sledeći kriterijumi:

- Rezultati merenja koji su:
 - o razumljivi,
 - o pravovremeno prezentovani, i
 - o objektivni, uporedivi i ponovljivi.
- Uspostavljeni procesi za dobijanje rezultata merenja, koji su:
 - o dobro definisani,
 - o jednostavni za rad i
 - o dobro praćeni.
- Rezultati merenja koji su korisni za unapređenje zaštite informacija; i
- Rezultati merenja koji odgovaraju informacionim potrebama.

2.8.2 Nadzor, preispitivanje i evaluacija programa merenja zaštite informacija

Nadzor, preispitivanje i evaluacija programa merenja zaštite informacija vrši se prema prethodno ustanovljenim kriterijumima (2.8.1)

Organizacija treba da identifikuje potencijalne potrebe za unapređenje:

- Programa merenja zaštite informacija, što podrazumeva:
 - o preispitivanje ili uklanjanje usvojenih konstrukcija merenja koji više ne odgovaraju i
 - o realokaciju resursa programa merenja zaštite informacija.
- Implementiranog sistema zaštite, uključujući područje primene, politike, ciljeve, kontrole, procese i procedure, kao i dokumentovanih odluka rukovodstva kako bi se omogućila uporedivost i analiza trendova u toku narednih preispitivanja.

Rezultati ovih evaluacija i identifikovanih potencijalnih potreba za unapređenja saopštavaju se zainteresovanim stranama, radi donošenja odluka za neophodna unapređenja. Organizacija treba da obezbedi način prikupljanja povratnih informacija od zainteresovanih strana. Povratne informacije predstavljaju jedan od ulaza za merenje efektivnosti programa merenja zaštite informacija.

2.8.3 Implementacija unapređenja

Povratne informacije zainteresovanih strana ukazuju na potrebe za unapređenjem programa merenja zaštite informacija. Identifikovana unapređenja moraju biti odobrena od strane rukovodstva, a planovi unapređenja moraju biti dokumentovani i saopšteni zainteresovanim stranama.

Veoma je bitno obezbediti da se implementacija unapređenja programa merenja zaštite informacija obavlja prema planu, za šta se mogu koristiti tehnike upravljanja projektima.

3 STUDIJA SLUČAJA: USPOSTAVLJANJE KAPACITETA ZA MERENJE UTICAJA BEZBEDNOSNIH RIZIKA

3.1 Uvod

Od svih tipova merenja performansi zaštite informacija (implementacija, efektivnost, efikasnost i uticaj), proces merenja uticaja zahteva najviši nivo zrelosti (Slika 2). Pošto ovaj proces koristi rezultate procesa koji su uključeni u upravljanje bezbednosnim rizikom, potrebno je da i oni imaju velike kapacitete za obezbeđenje automatizovanog prikupljanja mernih podataka. Prema tome, prvo treba uspostaviti i izmeriti kapacitete i zrelost svih procesa čije će izlazne informacije biti korišćene u procesu merenja uticaja, uključujući i sam proces merenja uticaja, što će biti opisano i demonstrirano u ovom poglavlju.

Merenje efektivnosti sistema upravljanja zaštitom informacija i implementiranih kontrola zaštite informacija, jedan je od osnovnih zahteva međunarodnog standarda ISO/IEC 27001, dok metod merenja performansi tih efektivnosti opisuje standard ISO/IEC 27005, što je, kako se vidi na Slika 2, nedovoljno za merenje performansi bezbednosnog uticaja na sistem. Ovakvu vrstu merenja opisuje američki nacionalni institut za standarde i tehnologiju, u svojoj specijalnoj publikaciji SP800-55, [5], a kao preduslov za merenje uticaja zahteva da procesi budu ponovljivi, procedure agilne, podaci uređeni u standardnim repozitorijumima i da se automatski prikupljaju u svrhe merenja. Ovo znači, da i sam proces merenja uticaja, kao i procesi koji obezbeđuju podatke, moraju da se podignu na viši nivo zrelosti, za šta se može iskoristi međunarodni standard ISO/IEC 21827, koji nudi model sazrevanja procesa zaštite. Za podršku u merenju zrelosti i poboljšavanju kapaciteta procesa zaštite, odabran je *Appraisal Assistant*, softverski proizvod australijskog instituta *Software Quality Institute (SQI)*¹³.

U PRILOG E, opisani su koraci modifikacije i korišćenja aplikacije “Appraisal Assistant”, za uspostavljanje kapaciteta merenja bezbednosnog uticaja na poslovanje.

3.2 Uspostavljanje kapaciteta merenja uticaja bezbednosnog rizika

Uticaj je posledica neželjenog incidenta, namerno ili slučajno izazvanog, koji ima štetan uticaj po imovinu. Direktnе posledice mogu biti destruktivne za određenu imovinu, šteta za IT sistem i gubitak poverljivosti, integriteta, raspoloživosti, kontrolisane odgovornosti, autentičnosti ili pouzdanosti. Indirektnе posledice mogu biti finansijski gubici, gubici na tržištu, gubitak ugleda i reputacije organizacije.

Merenje uticaja omogućava da se izbalansiraju posledice neželjenog incidenta sa troškovima kontrole rizika, odnosno zaštite od incidenta. Takođe, uzima se u obzir i frekvencija pojave neželjenog događaja, što je posebno važno kada su male posledice (cena) pojedinačnog neželjenog događaja, ali i agregirani efekat većeg broja incidenata koji su se desili u određenom vremenskom periodu, koji takođe može biti štetan. Procena uticaja je važan element procene rizika i izbora mera zaštite.

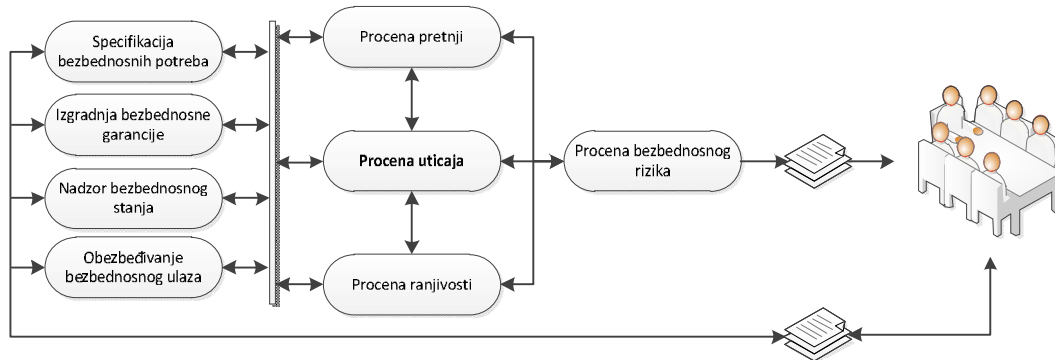
3.2.1 Procena uticaja

U ovom procesu se identifikuju uticaji koji su od interesa za sistem i procenjuje verovatnoća nastanka štetne posledice. Uticaji mogu biti opipljivi, kao što su gubitak prihoda ili novčane kazne, ili neopipljivi, poput gubitka reputacije i ugleda. Od svih procesa koji su uključeni u upravljanje bezbednosnim rizikom, procena uticaja je

¹³ [Software Quality Institute, Griffith University](http://www.sqi.org.au)

najzahtevniji proces. Informacije koje generiše ovaj proces, koriste se u procesima procene pretnji i ranjivosti informacione imovine (i obrnuto), a zajedno obezbeđuju ulazne informacije za proces procene bezbednosnog rizika.

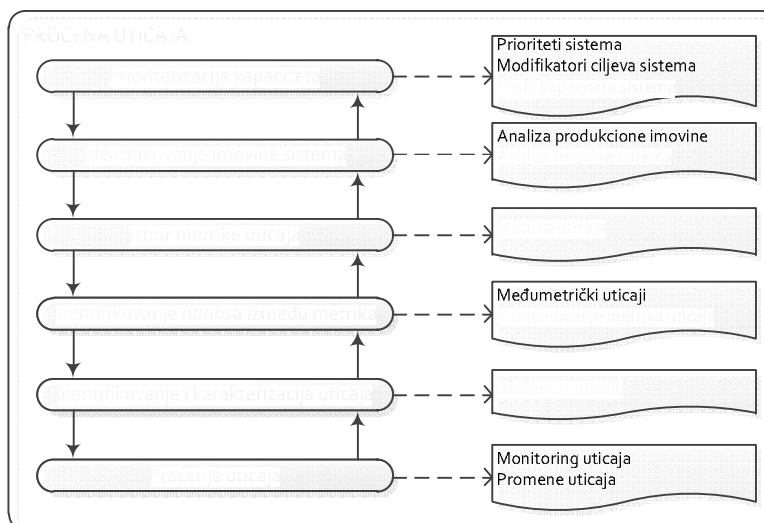
Iako su aktivnosti analize pretnji, ranjivosti i uticaja grupisane u različite oblasti procesa, one su međusobno zavisne. Cilj je da se pronađe kombinacija pretnji, ranjivosti i uticaja, koja je dovoljno rizična da opravda preduzimanje akcija za ublažavanje rizika. Prema tome, procena uticaja treba, u određenoj meri, da se vodi postojanjem odnosnih pretnji, ali i informacijama iz ostalih procesa upravljanja rizikom. Zato je, za uspostavljanje procesa merenja uticaja, potrebno identifikovati ili uspostaviti sve procese koji razmenjuju informacije sa ovim procesom, što je ilustrovano na Slika 10.



Slika 10 Tokovi informacija između procesa upravljanja rizikom

Pošto su uticaji podložni promenama, moraju periodično da se prate i preispitivaju, kako bi se u svakom trenutku očuvalo razumevanje i konzistentnost informacija koje generiše ovaj proces.

Cilj procesa procene uticaja je da se identifikuju i karakterizuju uticaji bezbednosnih rizika na sistem, što se postiže inženjerskim praksama ilustrovanim na Slika 11 i opisanim u narednom tekstu.



Slika 11 Proces procene uticaja

Prioritetizacija kapaciteta sistema

U ovoj praksi se vrši identifikovanje, analiza i prioritetizacija operativnih, poslovnih ili strateških kapaciteta sistema. Ona je u čvrstoj vezi sa aktivnostima procesa specifikacije bezbednosnih potreba.

Procena uticaja podrazumeva prioritetizaciju ostvarenja operativnih, poslovnih ili strateških ciljeva, koji su u vezi sa predmetom procene, odnosno, prioritetizaciju rizika tretiranih u drugim praksama i procesima. Zato, prilikom ispitivanja potencijalnih uticaja, neophodno je proceniti faktore koji mogu uticati na te prioritetne ciljeve.

Odabrani metod procene rizika treba da definiše način vrednovanja i prioritetizacije kapaciteta i imovine. Funkcionalna i informaciona imovina (PRILOG D) može da se predstavi svojom vrednošću i kritičnošću u definisanom okruženju. Vrednost može da se predstavi operativnim značajem, klasifikacijom, nivoom osetljivosti, ili bilo kojim drugim načinom utvrđivanja vrednosti imovine koja se koristi u sistemu. Kritičnost može da se predstavi uticajem na systemske operacije, ljudski život, operativne troškove, kao i drugim faktorima kritičnosti u situacijama kompromitacije, promene, ili nedostupnosti funkcija operativnog okruženja. Imovina takođe može biti definisana u odnosu na bezbednosne zahteve. Na primer, imovina može da se definiše poverljivošću baze klijenata, raspoloživošću kancelarijskih komunikacija, ili integritetom platnih spiskova. Većina imovine je uglavnom neodređena ili nejasno definisana.

Aktivnosti prioritetizacije kapaciteta sistema, na osnovu bezbednosnih potreba, vrednosti i značaja funkcionalne i informacione imovine, daju listu prioriteta i modifikatora ciljeva sistema, kao i konačan profil kapaciteta sistema, gde su opisani kapaciteti sistema i njihov značaj za ostvarenje ciljeva sistema.

Identifikovanje imovine sistema

Aktivnosti ove prakse su usmerene na identifikovanje i karakterizaciju sistemskih resursa, koji služe kao sredstva za podršku ključnih kapaciteta sistema (operativnih, poslovnih ili onih koji su u funkciji misije) za ostvarenje bezbednosnih ciljeva sistema. Sredstva za podršku se definišu procenom njihovog značaja unutar definisanog okruženja.

Najopštija podela informacione imovine podrazumeva ljude, okruženje i infrastrukturu sistema, uključujući podatke i ostale resurse koji nisu tipično informacioni, ali su takođe

sistemske (npr. komunikaciona sredstva, podaci prikupljeni u svrhu istraživanja, aplikacije i štampači). Značaj ovih sredstava može da se interpretira njihovim doprinosom kapacitetima posmatranog okruženja. Imovina ne mora obavezno da bude deo bezbednosnih mehanizama; ona može da pripada i nezaštitnim mehanizmima podrške bezbednosnih funkcija ili mehanizama zaštite.

U nekim slučajevima, ova praksa preispituje aktivnosti procesa obezbeđivanja bezbednosnog ulaza i verifikacije i validacije zaštite. Kao rezultat njenih aktivnosti, dobijaju se izveštaji analize produkcione imovine i imovine sistema, koji sadrže listu produkcione i sistemske imovine i njihov značaj za funkcionisanje sistema.

Izbor metrike uticaja

Za merenje uticaja bezbednosnih događaja mogu da se koriste razne metrike. Najbolje je unapred odrediti koja metrika treba da se koristi za posmatrani deo sistema.

Ograničavanjem broja konzistentnih metrika, smanjuje se kompleksnost i problemi prilikom korišćenja više različitih metrika. Kvantitativna i kvalitativna merenja uticaja mogu da se izvedu na različite načine, kao što su: izrada finansijskih troškova; empirijsko skaliranje jačine uticaja, npr. od 1 – 10; i korišćenje predefinisanih prideva, npr. nizak, srednji, visok.

Identifikovanje odnosa među metrikama

Ovde se vrši identifikovanje odnosa među odabranim metrikama procene uticaja i, ako je potrebno, identifikovanje metričkih faktora konverzije.

Različiti uticaji se procenjuju različitim metrikama. Da bi se u toku procene uticaja obezbedio konzistentan pristup svim izloženostima, moraju da se utvrde veze između različitih metrika. U nekim situacijama potrebno je kombinovati metrike, kako bi se dobio jedinstven konsolidovan pokazatelj uticaja. Zbog toga, treba uspostaviti pristup za konsolidaciju, koji obično varira u zavisnosti od prirode posmatranih sistema.

Kada se koriste kvalitativne metrike, takođe treba uspostaviti pravila koja će da usmeravaju kombinovanje kvalitativnih faktora u fazi konsolidacije. Kao primer izloženosti može da se uzme meteor koji može da uništi kuću, jedan potencijalni uticaj su troškovi izgradnje kuće, od, npr. 100,000€, dok drugi uticaj može da bude gubitak smeštaja od 6 meseci do ponovne izgradnje kuće. Ova dva uticaja mogu da se kombinuju sa mesečnom cenom smeštaja od 250€, pa bi ukupan uticaj za ovu izloženost meteoru bio 101,500€.

Tipične informacije koje generiše ova praksa su lista međumetričkih uticaja, gde su opisane relacije među odabranim metrikama, i pravila za kombinovanje metrika uticaja.

Identifikovati i karakterizacija uticaja

Identifikovanje i karakterizacija štetnih posledica neželjenih incidenata, vrši se upotrebom posebne metrike ili konsolidacijom pokazatelja različitih metrika, a kao rezultat dobija se lista izloženosti uticaju, koja sadrži spisak potencijalnih uticaja i odnosnih metrika.

Nakon identifikovanja imovine i kapaciteta, u praksama prioritizacije kapaciteta sistema i identifikovanja imovine sistema, ovde treba identifikovati štetne posledice za svaku imovinu, uključujući njeno oštećenje, otkrivanje, opstrukciju ili gubljenje. Neželjeni uticaji na kapacitete mogu biti uzrokovani prekidom, kašnjenjem ili slabljenjem zaštite.

Izrada liste štetnih posledica uzrokovanih neželjenim incidentima, oslanja se na metrike identifikovane prilikom izbora metrika uticaja i identifikovanja njihovih međusobnih

odnosa, statistička istraživanja i druge relevantne izvore. Pored toga, svakom uticaju se pridružuje stepen neodređenosti u metrikama.

Procena uticaja se vrši na osnovu metrika uticaja utvrđenih prilikom izbora metrike uticaja, a uticaji se kombinuju prema pravilima uspostavljenim aktivnostima prakse identifikovanja odnosa među metrikama. U većini slučajeva postoje izvesne neodređenosti u metrikama i verovatnoći da će se neki uticaj desiti u određenom okruženju. Generalno, mnogo je efektivnije držati faktore neodređenosti razdvojene od same metrike, tako da, kada se vrši precizna obrada radnih podataka, može da se utvrdi da li je rezultat sam podatak ili kombinacija neodređenosti koja prati podatak.

Praćenje uticaja

Pošto su svi uticaji koji su identifikovani na određenim lokacijama su dinamični, treba redovno pratiti tekuće promene uticaja. Takođe, pošto novi uticaji uvek mogu postati relevantni, pored redovnog praćenja promena postojećih uticaja, treba identifikovati i potencijalne uticaje. Ova praksa je usko povezana sa opštim aktivnostima praćenja promena bezbednosnog stanja, koje pripadaju procesu nadzora bezbednosnog stanja.

Rezultat praćenja promena predstavlja se u formi izveštaja o rezultatima monitoringa uticaja i promenama uticaja, gde su detaljno opisane promene na uticajima.

Pošto su uticaji promenjivi, procena uticaja treba da bude iterativna i da se u određenom okruženju obavezno obavlja više puta. Treba imati u vidu, da ponovne procene uticaja ne mogu biti zamena za redovno praćenje uticaja.

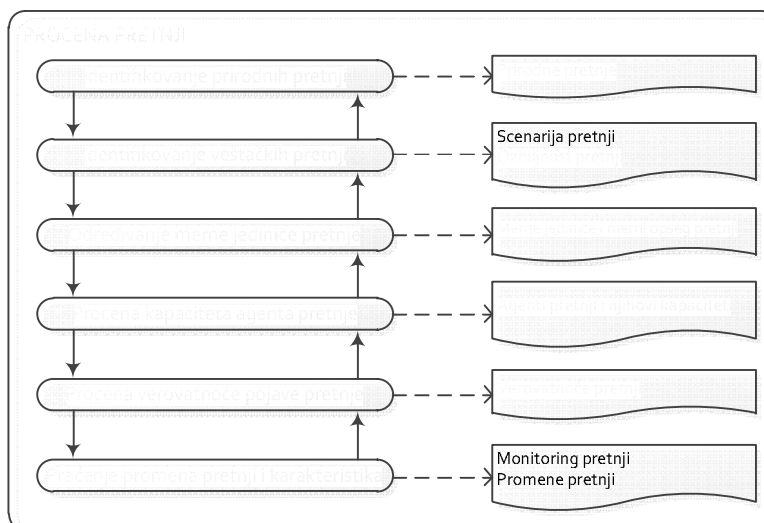
3.2.2 Procena pretnji

U procesu procene pretnji vrši se identifikovanje bezbednosnih pretnji i njihovih osobina, u cilju dobijanja liste pretnji sa svim definisanim karakteristikama, koja će se koristiti u ostalim procesima koji su uključeni u upravljanje bezbednosnim rizikom.

Za procenu pretnji mogu da se koriste razni pristupi i metodologije, ali je najbitnije prethodno utvrditi veze odabrane metodologije sa metodologijama koje se koriste u ostalim aktivnostima procene rizika. Zbog međusobne zavisnosti procesa procene pretnji, ranjivosti i uticaja, otkrivanje pretnji treba, u određenoj meri, da se oslanja na identifikovane odnosne ranjivosti i uticaje.

Pošto su pretnje takođe podložne promenama, moraju periodično da se prate i preispitavaju, kako bi se u svakom trenutku očuvalo razumevanje i konzistentnost informacija koje generiše ovaj proces.

Cilj procesa procene pretnji je da se identifikuju i karakterizuju pretnje, koje mogu biti upotrebljene od strane agenta pretnji i iskoristiti ranjivost mete napada, što se postiže inženjerskim praksama ilustrovanim na Slika 12 i opisanim u narednom tekstu.



Slika 12 Proces procene pretnji

Identifikovanje pretnji koje su posledica aktivnosti čoveka

Ovde treba identifikovati primenjive pretnje koje su posledica aktivnosti čoveka, bilo namernih ili slučajnih.

Pretnje koje su posledica aktivnosti čoveka zahtevaju malo drugačiji tip pristupa. U osnovi, postoje dva tipa veštačkih pretnji: one čiji je izvor namarena aktivnost i one koje su posledica slučajne aktivnosti. Neke veštačke pretnje ne mogu da se primene na posmatrano okruženje, te njihovo razmatranje odmah treba eliminisati iz tekućih analiza.

U nekim slučajevima, da bi se doprinelo razumevanju namernih pretnji, treba izraditi scenario koji opisuje kako pretnja može nastati. Kada se koristi generička baza veštačkih pretnji, treba razmotriti njihovu kompletnost (preciznost) i relevantnost (primenjivost).

Rezultat aktivnosti ove prakse su opisi scenarija pretnji, odnosno načina funkcionisanja pretnji, i rezultati procene ozbiljnosti pretnji, koji su dobijeni merenjem verovatnoće pojave pretnji.

Određivanje merne jedinice pretnje

Za svaku kategoriju pretnji treba identifikovati odgovarajuću mernu jedinicu i merne opsege primenjive u posmatranom okruženju.

Većina prirodnih i veštačkih pretnji već imaju jedinicu mere. Jedan od primera je Rihterova skala jačine zemljotresa. U većini slučajeva ukupan opseg mernih jedinica primenjiv je samo na određenu lokaciju. Zato je korisno uspostaviti maksimum, a u nekim slučajevima i minimum, pojave događaja pretnje na posmatranoj lokaciji.

Kada merna jedinica određene pretnje ne postoji, ili nije primenjiva za posmatranu lokaciju, treba je kreirati, uspostaviti njen opseg i opisati tako da može da se testira, što se obično definiše u tabeli pretnji sa pridruženim mernim jedinicama i opsezima na lokacijama.

Procena kapaciteta agenta pretnje

Za sve pretnje koje potiču od aktivnosti čoveka, treba proceniti kapacitete i motivaciju agenta pretnje.

Procena pretnji se fokusira na utvrđivanje potencijalnih sposobnosti i kapaciteta čoveka da uspešno izvrši napad na sistem. Sposobnost se odnosi na znanje napadača (npr. da li je obučen i da li ima znanje i veštine). Kapacitet je mera verovatnoće da će protivnik zaista izvršiti napad (npr. da li imaju resurse).

Namerne pretnje su u velikoj zavisnosti od sposobnosti i raspoloživih resursa agenta pretnje. Relativno iskusan haker koji ima pristup hakerskim alatima, može biti mnogo veća pretnja od iskusnog i sposobnog hakera, ali ne i toliko opasna kao pretnja iza koje stoji iskusan haker. Neiskusan haker može slučajno napraviti ogromnu štetu, dok je manja verovatnoća da će je napraviti iskusan haker, koji tačno radi ono šta mu je namera. Pored sposobnosti agenta pretnje, procena vrednosti imovine kojima agent može pristupiti, treba da uključi procenu njegove motivacije i koliko je imovina za njega atraktivna.

Da bi postigao svoj cilj, agent pretnje može izvršiti veliki broj više uzastopnih napada, ili više različitih napada odjednom. Efekat ovih napada treba da se razmotri i da se izrade njihova scenarija. Kranji rezultat ove prakse je opis agenata pretnji, koji sadrži procenu i opis njegovih kapaciteta.

Procena verovatnoće pojave pretnje

Prilikom procene verovatnoće da će se ostvariti pretnja, treba razmotriti razne faktore. Od šanse da će se ostvariti prirodna pojava pretnje, do namernog ili slučajnog delovanja pojedinca. Mnogi od ovih faktora sami po sebi ne vode do jasnog rezultata ili mere. Za procenu pojave događaja pretnje potrebna je konzistentna metrika izveštavanja.

Procena verovatnoće pojave pretnje je komplikovana kalkulacija, jer mnoge promenjive uključuju različite verovatnoće. U svakoj proceni verovatnoće prisutan je faktor neodređenosti i validnosti procene. Da bi se ublažile potencijalne zabune i nesporazumi, faktore neodređenosti procene verovatnoće treba držati odvojeno od kalkulacije koja ne uključuje neodređenost, tako da uvek može da se iskoristi za preciznije dobijanje rezultata.

Rezultat ovih aktivnosti je izveštaj verovatnoće realizacije pretnji, koji za svaku identifikovanu pretnju sadrži opis verovatnoće njene pojave.

Identifikovanje prirodnih pretnji

Cilj ove prakse je da se identifikuju pretnje koje potiču iz prirodnih izvora, a primenjive su na posmatranoj lokaciji ili unutar definisanog okruženja sistema.

Pretnje koje potiču iz prirodnih izvora mogu biti zemljotres, cunami i tornado, ali nisu sve prirodne pretnje primenjive na sve lokacije. Na primer, cunami ne može da se desi u centru velikog kontinenta, ako može, onda je to smak sveta. Zato je važno identifikovati koje prirodne pretnje postoje na određenoj lokaciji.

Većina informacija za ovu procenu može da se preuzme iz statističkih arhiva i podataka o prirodnim fenomenima. Iako su ove informacije korisne, treba ih oprezno koristiti, jer su veoma generalizovane i zato treba da se tumače da predstavljaju specifično okruženje, a ne globalno, na primer, godišnja površina odronjavanja zemljišta u Srbiji je oko 2000 hilj.ha, ali je pitanje da li se odroni odnose na posmatrano okruženje.

Kada se identifikuju sve primenjive prirodne pretnje, kreira se tabela pretnji, u kojoj se pored liste prirodnih pretnji dokumentuje njihov karakter i verovatnoće pojave.

Praćenje promena pretnji i njihovih karakteristika

Pošto je spektar pretnji, koji je primenjiv na neku lokaciju i situacije, dinamičan, vremenom nove pretnje mogu postati relevantne, kao i promene karakteristika postojećih pretnji. Zato je važno pratiti postojeće pretnje i njihove karakteristike i redovno

proveravati postojanje novih pretnji. Ova praksa je, kao i ostale prakse monitoringa promena, deo opšte prakse praćenja promena bezbednosnog stanja koja pripada procesu nadzora bezbednosnog stanja.

Pošto su pretnje promenjive, procena pretnji treba da se obavlja više puta u posmatranom okruženju, ali ponavljanje procene pretnji ne sme biti zamena za aktivnosti praćenja pretnji.

Pošto se pretnje menjaju tokom vremena, procenu pretnji treba redovno obavljati u posmatranom okruženju, ali, kao i u slučaju redovne provere promena uticaja, ponovne procene pretnji ne mogu biti zamena za redovno praćenje promena pretnji.

Rezultati praćenja promena pretnji i njihovih karakteristika, evidentiraju se u izveštajima rezultata monitoringa promena u pretnjama i spektrima pretnji.

3.2.3 Procena ranjivosti

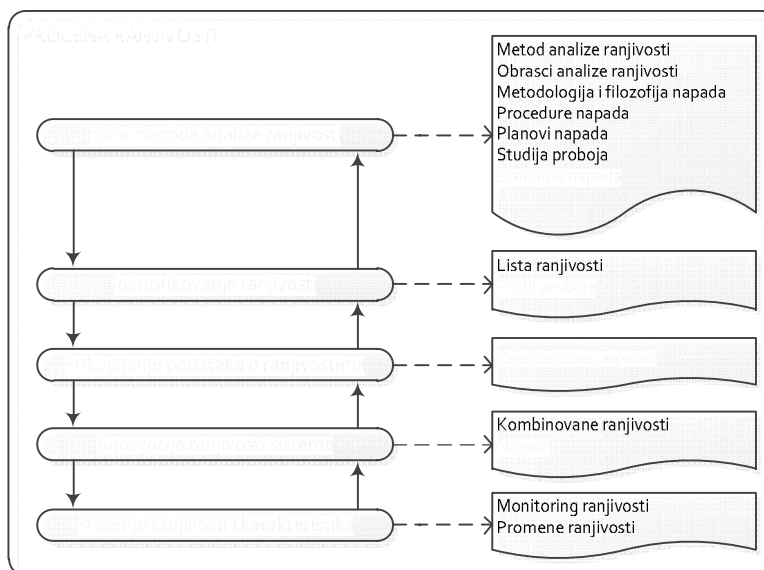
Procena ranjivosti treba da identifikuje i okarakterise bezbednosne ranjivosti sistema, što podrazumeva analizu imovine sistema, definisanje specifičnih ranjivosti i procenu celokupne ranjivosti sistema. Ranjivost, kao pojam, odnosi se na svojstvo sistema da se može koristiti u nenamenske svrhe, da ima slabosti, bezbednosne rupe, ili greške u implementaciji koje mogu biti napadnute (iskorišćene/zloupotrebljene) određenim pretnjama. Ove ranjivosti su nezavisne od bilo koje pojedinačne pretnje ili napada. Aktivnosti procene ranjivosti vrše se neprekidno u životnom ciklusu sistema, radi podrške donošenju odluka u razvoju, održavanju i operativnom radu sistema u posmatranom okruženju.

Analize i prakse ovog procesa, uglavnom su studije papirološke prirode. Otkrivanje ranjivosti sistema pomoću aktivnih alata i tehnika jeste drugi metod, ali on samo dopunjava analitičke tehnike. Ove aktivne tehnike mogu da se posmatraju kao specijalizovani oblik analize ranjivosti, koji može da se koristi za validaciju bezbednosne ranjivosti sistema nakon primene velikih nadogradnji sistema, ili za identifikovanje ranjivosti u situacijama međusobnih povezivanja sistema. U nekim situacijama, aktivna analiza ranjivosti služi za validaciju bezbednosnog stanja sistema i da se unapredi percepcija i razumevanje postojećih bezbednosnih ranjivosti. Aktivna analiza ranjivosti po nekad može da bude testiranje otpornosti (neprobojnosti) sistema, kada inženjeri zaštite pokušavaju da zaobiđu bezbednosne funkcije sistema, tako što rade pod istim uslovima kao obični korisnik, ali za razliku od običnih korisnika, pretpostavlja se da raspolažu dokumentacijom dizajna i implementacije sistema. Proces napada na zaštitu praktično je beskonačan i vremenski i finansijski ograničen.

Informacije koje generiše ovaj proces koriste se u procesu procene bezbednosnog rizika, koji takođe koristi izlazne informacije procesa procene pretnji i uticaja. Prema tome, otkrivanje ranjivosti treba, u određenoj meri, da se rukovodi postojanjem odnosnih pretnji i uticaja.

Pošto su ranjivosti podložne promenama, moraju periodično da se prate i preispitivaju, kako bi se u svakom trenutku očuvalo razumevanje i konzistentnost informacija koje generiše ovaj proces.

Cilj ovog procesa je da se, kod svih relevantnih učesnika, postigne razumevanje bezbednosnih ranjivosti sistema u okviru definisanog okruženja, što se postiže inženjerskim praksama ilustrovanim na Slika 13 i opisanim u narednom tekstu.



Slika 13 Proces procene ranjivosti

Izbor metoda analize ranjivosti

Cilj ove prakse je da se odaberu metode, tehnike i kriterijumi po kojima će, u definisanom okruženju sistema, ranjivosti biti analizirane, procenjivane, upoređivani i prioritetizovani. Definisanje metoda identifikovanja i karakterizacije bezbednosnih ranjivosti sistema, koji sadrži šeme kategorizacije i prioritetizacije ranjivosti, vrši se na osnovu pretnji i njihove verovatnoće, operativnih funkcija, bezbednosnih zahteva, ili drugih oblasti od interesa. Identifikovanje nivoa detalja, odnosno, intenziteta, dubine i obima analize, inženjerima zaštite i korisnicima sistema daje do znanja koji deo sistema će biti predmet posmatranja. Analiza treba da se izvršava u okviru poznate i snimljene konfiguracije, u unapred dogovorenom i utvrđenom vremenskom periodu. Metodologija analize treba da sadrži očekivane rezultate i da jasno navodi specifične ciljeve.

Metod analize ranjivosti može biti postojeći, prilagođen, ili specifičan za operativne aspekte i posmatrano okruženje sistema. Često se zasniva na metodologiji analize rizika (ili je dopunjuje) odabranoj u procesu procene bezbednosnog rizika. Treba imati u vidu da metodologija ne mora da obezbedi razumevanje o pretnjama, kapacitetima agenata pretnji i vrednostima imovine, što sužava njen delokrug i pojednostavljuje upotrebu.

Za identifikovanje ranjivosti postoje dva različita pristupa, analitički i testni. Pristup koji se zasniva na testiranju je dobar za identifikovanje ranjivosti za koje već postoji skup poznatih pretnji uključenih u testnu bazu. Analitički pristupi su najbolji za identifikovanje novih ranjivosti i onih koji trenutno nisu dostupni za eksploataciju, ali koji mogu biti na raspolaganju kada se iskoristi druga ranjivost. Ostale opcije koje mogu da se razmatraju prilikom izbora metodologije procene ranjivosti, uključuju kvalitativne i kvantitativne pristupe. Takođe treba uzeti u obzir i kontrolu kompletnosti analize ili testiranja. Rezultati aktivnosti ove prakse su:

- Metod analize ranjivosti – pristup za pronalaženje bezbednosnih ranjivosti sistema, uključujući postupak analize, izveštavanja i praćenja.
- Obrasci analize ranjivosti – definisani obrasci vođenja rezultata analize ranjivosti, kako bi se obezbedio standardizovan pristup.
- Metodologija i filozofija napada – ciljevi i pristup testiranja napadom.

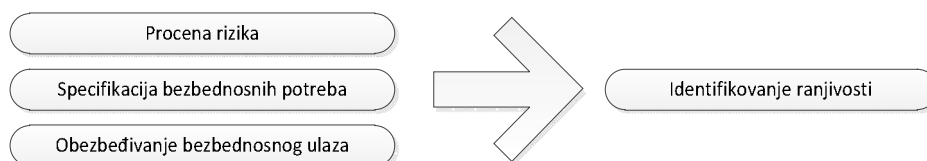
- Procedure napada – detaljan opis koraka izvođenja testiranja napadom.
- Planovi napada – uključuju resurse, dinamički plan i opis metodologije napada.
- Studija proboja – analiza i izrada scenarija napada za identifikovanje nepoznatih ranjivosti.
- Scenarija napada – opis specifičnih napada koji će biti isprobani.

Identifikovanje ranjivosti

Bezbednosne ranjivosti sistema mogu da se pronađu u bezbednosnim i nebezbednosnim delovima sistema. U većini slučajeva, otkrije se da nebezbednosni mehanizmi koji podržavaju bezbednosne funkcije, ili rade u sprezi sa bezbednosnim mehanizmima, imaju ranjivosti koje se mogu zloupotребiti. Metodologija scenarija napada, razvijena u prethodnoj praksi, treba da prati meru validacije ranjivosti. Sve otkrivene ranjivosti sistema moraju biti dokumentovane.

U ovoj praksi, ranjivosti se posmatraju kao funkcija sistema, bez razmatranja verovatnoće bilo kakve pretnje. Redosled ovakvih ranjivosti može da se prioritetizuje u toku analize pretnji. Napadi koji nisu ponovljivi otežavaju posao razvoja zaštite.

Na Sliku 14, prikazano je da se identifikovanje ranjivosti oslanja na informacije prioriteta ranjivosti, koji su identifikovani u procesu procene rizika i u procesu specifikacije bezbednosnih potreba, prilikom identifikovanja poslovnih prioriteta i ciljeva. Pored toga, identifikovanje ranjivosti uzima u obzir informacije o imovini, koje su dobijene od procesa obezbeđivanja bezbednosnog ulaza za inženjerske aktivnosti sistema.



Slika 14 Bezbednosni ulazi za identifikovanje ranjivosti

Rezultati ove prakse dokumentuju se u listi ranjivosti, gde se opisuju ranjivosti sistema na različite napade, i izrađuju profili proboja sa rezultatima testiranja ranjivosti napadom.

Prikupljanje podataka o ranjivostima

Svaka ranjivost ima određena svojstva. U ovoj bazičnoj praksi prikupljaju se svi podaci koji se odnose na osobine ranjivosti. Po nekad, ranjivosti mogu imati jedinicu mere sličnu pretnjama. Treba identifikovati i dokumentovati lakoću kojom se može iskoristiti ranjivost i verovatnoću pojave ranjivosti.

Većina podataka prikupljenih tokom ovih aktivnosti, kasnije se koriste u procesu procene bezbednosnih rizika. Zato je važno prikupljene podatke skladištiti u formatu upotrebljivom za proces procene bezbednosnih rizika.

Pošto i u ovom slučaju, kao u slučaju procene pretnji i uticaja, postoje izvesne neodređenosti u metrikama i verovatnoćama, mnogo je efektivnije faktore neodređenosti razdvojiti od same metrike, tako da, kada se vrši precizna obrada radnih podataka može da se utvrdi da li je rezultat sam podatak ili kombinacija neodređenosti koja prati podatak.

Rezultati prikupljanja podataka o ranjivostima vode se u tabeli osobina ranjivosti, gde se dokumentuju karakteristike ranjivosti proizvoda ili sistema.

Agregiracija ranjivosti sistema

Ovde je potrebno proceniti i analizirati koje su ranjivosti, ili njihove kombinacije, problematični za sistem i agregirati ranjivosti koje su rezultat kombinovanaj specifičnih ranjivosti. Analiza treba da identifikuje dodatne karakteristike ranjivosti, kao što je verovatnoća i mogućnost eksploatacije ranjivosti. Rezultati procene ranjivosti mogu da sadrže i preporuke za sintetizovanje ranjivosti.

Takođe, treba obezbediti rezultate analize i vežbi napada. Sve otkrivene ranjivosti i mogućnosti njihove eksploatacije, treba da budu identifikovani i dokumentovani sa dovoljno detalja potrebnih za donošenje odluke o protivmerama.

Na kraju, dokumentuju se izveštaji procene ranjivosti, koji sadrže kvantitativni i kvalitativni opis ranjivosti problematičnih za sistem, uzimajući u obzir verovatnoću napada, verovatnoću uspeha i uticaj napada, kao i izveštaji napada, gde se evidentiraju rezultati i analize otkrivenih ranjivosti, njihovih potencijalnih izloženosti i eventualne preporuke za ublažavanje ili otklanjanje ranjivosti.

Praćenje promena ranjivosti i njihovih karakteristika

Praćenje tekućih promena ranjivosti i njihovih karakteristika, dokumentuje se u izveštaju redovnog praćenja tekućih ranjivosti, kao i izveštajima gde se opisuju nove ranjivosti i promene u postojećim ranjivostima.

Spektar ranjivosti, koji je primenjiv na neku lokaciju i situacije, je dinamičan. Vremenom, nove ranjivosti mogu postati relevantne, kao i promene karakteristika postojećih ranjivosti. Zato je važno pratiti postojeće ranjivosti i njihove karakteristike i redovno proveravati prisustvo novih ranjivosti. Ova praksa je, kao i ostale prakse monitoringa promena, u tesnoj vezi sa praksom praćenja promena bezbednosnog stanja, koja pripada procesu nadzora bezbednosnog stanja i prati promene pretnji, ranjivosti, uticaja, rizika i okruženja.

Pošto su ranjivosti promenjive, procenu ranjivosti treba redovno obavljati u posmatranom okruženju, ali ponavljanje procene ranjivosti ne može da se smatra zamenom aktivnosti praćenja redovnog praćenja ranjivosti.

3.2.4 Procena bezbednosnog rizika

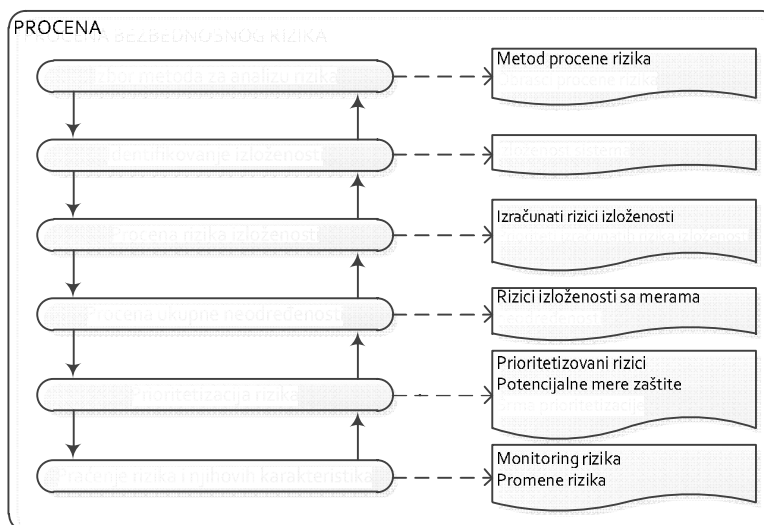
Procena bezbednosnog rizika identifikuje bezbednosne rizike sistema u određenom okruženju, metodom utvrđivanja rizika na osnovu poznavanja kapaciteta agenata pretnji, da iskoriste ranjivost imovine sistema. Konkretno, aktivnosti ovog procesa uključuju identifikovanje i procenu verovatnoće pojave izloženosti, koja predstavlja kombinaciju pretnji, ranjivosti i štetnih uticaja. Procena bezbednosnog rizika se neprekidno obavlja u životnom veku sistema, kada treba doneti odluku koja se odnosi na bezbedan razvoj, održavanje ili rad sistema.

Bezbednosni rizik je verovatnoća da će neželjeni incident izazvati štetne posledice. Projektni rizici uključuju troškove i dinamički plan, a bezbednosni rizici se bave zaštitom od štetnih uticaja na imovinu i kapacitet sistema. Procena rizika uvek uključuje faktor neodređenosti, koji varira u zavisnosti od situacije. Što znači, da uvek postoje određena ograničenja predviđanja verovatnoće. Uticaj koji se procenjuje za određeni rizik takođe ima svoje neodređenosti, jer uticaj neželjenog incidenta može izazvati neočekivane posledice. Prema tome, preciznost predviđanja uvek prati izvesni faktor neodređenosti, koji nekad može biti prilično velik, što komplikuje planiranje i opravdanost zaštite.

Uvek je korisno razmotriti sve što može da smanji neodređenost koja je prisutna u posmatranoj situaciji, jer se tada povećava bezbednosna garancija koja indirektno redukuje rizik. Informacije o riziku koje se dobijaju u ovoj oblasti procesa, zavise od informacija o

pretnjama, ranjivostima i uticajima. Iako su aktivnosti analize pretnji, ranjivosti i uticaja grupisane u različite oblasti procesa, one su međusobno zavisne. Cilj je da se pronađe kombinacija pretnji, ranjivosti i uticaja, koja je dovoljno rizična da opravda preduzimanje akcija. Ove informacije formiraju osnovu za definisanje bezbednosnih potreba i bezbednosnog ulaza.

Pošto je okruženje posmatranog rizika podložno promenama, ono mora periodično da se nadgleda i preispituje, kako bi se u svakom trenutku očuvalo razumevanje i konzistentnost informacija o rizicima koje generiše ovaj proces. Cilj ovog procesa je da se postigne razumevanje bezbednosnih rizika, koji se odnose na rad sistema unutar definisanog okruženja, i da se rizici prioritetizuju prema definisanoj metodologiji, što se postiže inženjerskim praksama ilustrovanim na Slika 15 i opisanim u narednom tekstu.



Slika 15 Proces procene bezbednosnog rizika

Izbor metoda za analizu rizika

Aktivnosti ove prakse usmereni su na izbor metoda, tehnika i kriterijuma po kojima će, u definisanom okruženju sistema, rizici biti analizirani, procenjivani, poređeni i prioritetizovani.

Identifikovanje, analiza, procena i poređenje bezbednosnih rizika sistema u određenom okruženju, vrši se definisanom metodom. Takođe, ovde se koriste šeme kategorizacije i prioritetizacije rizika, na osnovu pretnji, operativnih funkcija, sistemskih ranjivosti, potencijalnih gubitaka, bezbednosnih zahteva i drugih oblasti koji su od interesa.

Metod može biti postojeći, prilagođen, ili specifičan za operativne aspekte i posmatrano okruženje sistema. Metodologija procene rizika treba da ima vezu i da bude konzistentna sa metodologijama procene pretni, ranjivosti i uticaja. Kao rezultat ove prakse dobija se:

- Metod procene rizika – pristup za identifikovanje i karakterizaciju rizika.
- Obrasci procene rizika – obrazac po kojem se rizici dokumentuju i prate, uključujući opis, značaj i zavisnosti.

Identifikovanje izloženosti

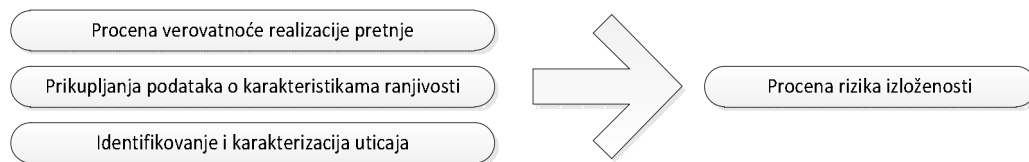
Cilj ove prakse je da se identifikuje izloženost pretnjama, ranjivostima i uticaju, što ovu praksu čini zavisnom od rezultata procesa procene pretnji, ranjivosti i uticaja. Svrha identifikovanja izloženosti je da se prepozna koje su pretnje i ranjivosti od interesa i da se

identifikuje uticaj iskorišćenja ranjivosti od strane pretnje. Identifikovane izloženosti vode se u listi izloženosti sistema, zajedno sa opisom svake izloženosti, a lista se koristi prilikom izbora zaštite sistema.

Procena rizika izloženosti

Procena rizika svake pojedinačne izloženosti, podrazumeva identifikovanje verovatnoće pojave izloženosti. Verovatnoća izloženosti je kombinacija verovatnoće pretnji i ranjivosti. Pošto se radi o verovatnoći specifičnog i generalizovanog obima ili težine uticaja, kao i u ostalim praksama procene verovatnoće, takođe postoji faktor neodređenosti korišćene metrike. I ovde se primenjuje preporuka da je mnogo efektivnije držati faktore neodređenosti razdvojene od same metrike, kako bi se koristili za precizna izračunavanja verovatnoće.

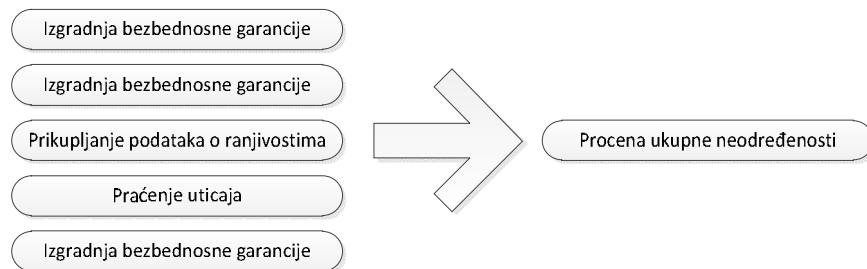
Da bi se procena uticaja realizacije izloženosti izvršila konsolidacijom postojećih metrika, procena izloženosti koristi podatke o verovatnoćama iz praksi procena verovatnoće realizacije pretnje, prikupljanja podataka o karakteristikama ranjivosti i identifikovanja i karakterizacije uticaja, što je ilustrovano na Slika 16. Na kraju, izrađuje se lista izračunatih rizika izloženosti i tabela prioriteta izračunatih rizika.



Slika 16 Bezbednosni ulazi za procenu uticaja realizacije izloženosti

Procena ukupne neodređenosti

Cilj ove prakse je da se proceni ukupna neodređenost rizika izloženosti, koja se evidentira u listi rizika koja prikazuje meru rizika i neodređenosti – *Rizici izloženosti i njihove neodređenosti*. Pošto svaki procenjeni rizik ima svoju neodređenost, ukupna neodređenost rizika je zbir neodređenosti za pretnje, ranjivosti, uticaje i njihove karakteristike, koje su identifikovane u praksama procene verovatnoće realizacije pretnje, prikupljanja podataka o karakteristikama ranjivosti, kao i praksi identifikovanja i karakterizacije uticaja koja se koristi za procenu uticaja izloženosti, što je ilustrovano na Slika 17. Ova praksa je usko povezana sa aktivnostima procesa izgradnje bezbednosne garancije, koje se mogu koristiti za modifikovanje, a u nekim slučajevima i redukovanje neodređenosti.



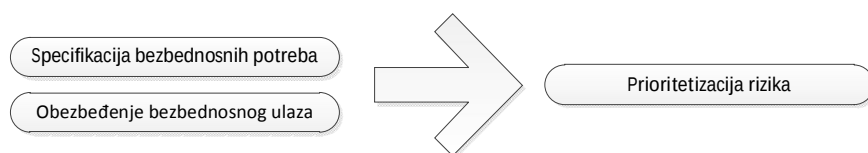
Slika 17 Bezbednosni ulazi za procenu ukupne neodređenosti rizika izloženosti

Ako se neodređenost ne posmatra odvojeno od verovatnoće pojave izloženosti, onda zaštitne mere mogu biti bespotrebno implementirane, jer u stvari nije bilo potrebe za tretiranjem rizika.

Prioritetizacija rizika

Sve identifikovane rizike treba sortirati prema prioritetima organizacije, verovatnoći pojave, neodređenosti i raspoloživim sredstvima. Rizik može biti ublažen, izbegnut (ukidanje rizične aktivnosti ili imovine), prenešen (odgovornost prepuštena drugoj organizaciji) ili prihvaćen. Takođe, moguća je kombinacija navedenih načina tretiranja rizika. Ublažavanje rizika može da tretira pretnje, ranjivost, uticaj ili sam rizik, što zavisi od potreba zainteresovanih strana, identifikovanih u procesu specifikacije bezbednosnih potreba, poslovnih prioriteta i celokupne arhitekture sistema.

Ovaj korak može biti veoma kompleksan, a često zahteva veći broj iteracija. Jedna zaštitna mera može da tretira više različitih rizika, ili pretnji, ranjivosti i uticaja, što može uticati na efektivnu prioritetizaciju rizika. Zato je ova oblast procesa u tesnoj vezi sa procesima specifikacije bezbednosnih potreba i obezbeđenja bezbednosnog ulaza, što je ilustrovano na Slika 18.



Slika 18 Bezbednosni ulazi za prioritetizaciju rizika

Rezultati aktivnosti ove prakse dokumentuju se u sledećem obliku:

- Lista prioriteta rizika – prioritetizovani rizici.
- Lista zahteva zaštitnih mera – lista potencijalnih mera zaštite koje mogu doprineti ublažavanju rizika.
- Obrazloženje prioritetizacije – opis šeme prioritetizacije.

Praćenje rizika i njihovih karakteristika

Praćenje tekućih promena rizika i njihovih karakteristika, dokumentuje se u izveštaju redovnog praćenja tekućih rizika, koji opisuju trenutni spektar rizika, i izveštajima gde se opisuju operativni kapaciteti sistema i njihov značaj za ciljeve sistema.

Spektar rizika na različitim lokacijama i situacijama je veoma dinamičan. Vremenom, novi rizici mogu postati relevantni, kao i promene karakteristika postojećih rizika. Zato je važno pratiti postojeće rizike i njihove karakteristike i redovno proveravati postojanje novih rizika. Ova praksa je, kao i ostale prakse monitoringa promena, u tesnoj vezi sa praksom praćenja promena bezbednosnog stanja, koja pripada procesu nadzora bezbednosnog stanja i prati promene pretnji, ranjivosti, uticaja, rizika i okruženja.

Pošto su rizici promenljivi, aktivnosti procene rizika mogu da se obavljaju više puta u posmatranom okruženju, ali ponavljanje procene rizika ne sme biti zamena za aktivnosti praćenja rizika.

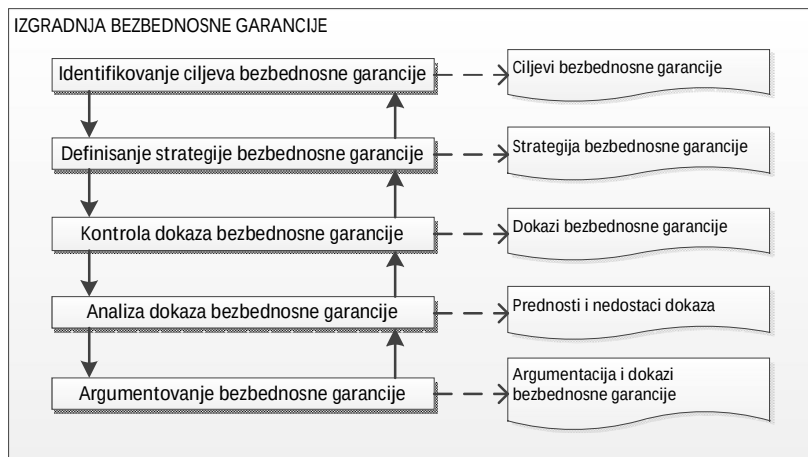
3.2.5 Izgradnja bezbednosne garancije

Namena procesa izgradnje bezbednosne garancije je da se jasno predstavi ostvarenje bezbednosnih potreba korisnika. Bezbednosna garancija je skup izjava o ciljevima garancije, podržani kombinacijom dokaza koji se mogu dobiti iz više različitih izvora i nivoa apstrakcije.

U ovom procesu se identifikuju i definišu zahtevi za bezbednosnim garancijama, aktivnosti izgradnje i analize dokaza, kao i dodatnih dokaza za podršku zahtevima za bezbednosnim

garancijama. Dokazi bezbednosne garancije se sortiraju, pakuju i pripremaju za prezentaciju.

Cilj ovog procesa je da se iz procesa i proizvoda rada organizacije prikupe jasni dokazi ispunjenja bezbednosnih potreba klijenta, što se postiže inženjerskim praksama ilustrovanim na Slika 19 i opisanim u narednom tekstu.



Slika 19 Proces izgradnje bezbednosne garancije

Identifikovanje ciljeva bezbednosne garancije

Ciljevi bezbednosne garancije uspostavljaju nivo poverenja u sistem prema zahtevima klijenta, ali na način koji neće narušavati zahteve politike bezbednosti sistema. Adekvatnost ciljeva određuje razvojni tim, integratori sistema i klijent. Identifikacijom novih i modifikacijom postojećih ciljeva bezbednosne garancije sistema, koordinira interna grupa za zaštitu, zajedno sa eksternim inženjerima zaštite (npr. klijent, certifikator sistema zaštite, korisnik).

Ciljevi bezbednosne garancije se redovno ažuriraju, kako bi pratili promene, kao što su: promene koje zahtevaju modifikaciju ciljeva bezbednosne garancije; promene nivoa prihvatljivog rizika klijenta, certifikatora sistema zaštite ili korisnika; ili promene u zahtevima i tumačenjima zahteva.

Ciljevi bezbednosne garancije moraju jasno i nedvosmisleno da se saopšte. Za bolju interpretaciju, mogu se koristiti grafičke i tabelarne metode prezentacije, odabrane prema zainteresovanim stranama (Tabela 8).

Tamo gde specifičan zahtev nije mandatoran, korisno je ostale ciljeve bezbednosne garancije povezati sa ispunjenjem tog zahteva, što će još jasnije opisati ciljeve i redukovati eventualne nejasnoće.

Kada se konačno postigne dogovor oko ciljeva bezbednosne garancije, dokumentuje se izjava o ciljevima bezbednosne garancije, koji su usmereni na ispunjenje zahteva klijenta za potrebnim nivoom poverenja u bezbednosne karakteristike sistema.

Definisanje strategije bezbednosne garancije

U ovom koraku definiše se strategija za ispunjenje svih ciljeva bezbednosne garancije. Dokument strategije bezbednosne garancije sadrži plan ispunjenja ciljeva bezbednosne garancije klijenta i identifikuje odgovorne učesnike za realizaciju plana.

Namena strategije bezbednosne garancije je da se planski obezbedi pravilna implementacija i primena bezbednosnih zahteva. Dokazi dobijeni u toku implementacije strategije bezbednosne garancije, treba da obezbede prihvatljiv nivo poverenja u adekvatnost mera zaštite sistema za upravljanje bezbednosnim rizicima. Efektivnost upravljanja aktivnostima bezbednosne garancije, postiže se razvojem i direktivama strategije bezbednosne garancije. Za dobijanje dodatnih dokaza, najbolje je u ranoj fazi identifikovati i definisati sve zahteve koji se odnose na bezbednosnu garanciju.

Viši nivo kvaliteta paketa bezbednosne garancije obezbeđuje se eksternom koordinacijom razumevanja i praćenja ispunjenja klijentskih potreba za bezbednosnom garacijom.

Koordinacija strategije bezbednosne garancije vrši se u okviru svih internih inženjerskih grupa, kao i eksternih grupa uključenih u poslovni proces (npr. klijenti, certifikator sistema zaštite, ili korisnici). Bezbednosnom koordinacijom se bavi poseban proces koordinacije zaštite, sa ciljem da:

- Svi članovi projektnog tima budu svesni i uključeni u aktivnosti bezbednosnog inženjeringa, u meri koja je neophodna za obavljanje njihovih funkcija; i
- Odluke i preporuke koje se odnose na bezbednost, budu saopštene i koordinisane.

Kontrola dokaza bezbednosne garancije

Cilj ove prakse je da se identifikuju i kontrolišu dokazi bezbednosne garancije. Dokazi se prikupljaju kako je definisano u strategiji bezbednosne garancije, kroz interakciju svih inženjerskih procesa zaštite, kako bi se identifikovali na različitim nivoima apstrakcije. Ovi dokazi moraju neprekidno da se kontrolišu, kako bi se očuvala njihova upotreba sa postojećim proizvodima rada, kao i njihova relevantnost za ciljeve bezbednosne garancije.

Dokazi bezbednosne garancije mogu da se dobiju iz sistema, arhitekture, dizajna, implementacije, inženjerskih procesa, fizičkog razvojnog i operativnog okruženja. Svi dokazi prikupljeni tokom razvoja, testiranja i operativnog rada, nalaze se u repozitorijumima dokaza bezbednosne garancije, koji mogu biti u formi baza podataka, inženjerski laptop, rezultati testiranja, ili dokazni logovi.

Analiza dokaza bezbednosne garancije

Analiza dokaza bezbednosne garancije je potrebna da bi se steklo uverenje da prikupljeni dokazi ispunjavaju bezbednosne ciljeve, odnosno, da zadovoljavaju bezbednosne potrebe klijenata. Analizom dokaza bezbednosne garancije utvrđuje se adekvatnost sistemskog bezbednosnog inženjeringa i procesa verifikacije zaštite, kako bi se ustanovilo da su uspešno implementirane bezbedne karakteristike i mehanizmi zaštite.

Pored toga, dokazi bezbednosne garancije se analiziraju kako bi se osigurala kompletnost i ispravnost inženjerskih artefakata u odnosu na osnovni sistem. U slučaju nekompletnih ili neadekvatnih dokaza bezbednosne garancije, ova analiza može zahtevati reviziju osnovnog sistema, bezbednosnih rezultata rada i procesa koji podržavaju bezbednosne ciljeve.

Neki dokazi bezbednosne garancije mogu da se generišu samo konsolidacijom ostalih sistem inženjerskih artefakata, ili izvesti konsolidacijom ostalih garancija. Rezultati analize dokaza bezbednosne garancije identifikuju i sumiraju prednosti i nedostatke dokaza, što se evidentira u repozitorijumu dokaza.

Argumentovanje bezbednosne garancije

Argumenti bezbednosne garancije pokazuju da su zadovoljene bezbednosne potrebe klijenta, a opisuju se u dokumentu argumentacije i dokaza bezbednosne garancije, koji

sadrži strukturiran skup ciljeva bezbednosne garancije podržan dokazima bezbednosne garancije.

Bezbednosnom argumentacijom se demonstrira usaglašenost sa ciljevima bezbednosne garancije, koji su usmereni na ispunjenje bezbednosnih zahteva klijenta. Bezbednosna garancija je skup izjava, koje sadrže ciljeve i dokaze bezbednosne garancije koji mogu biti predstavljeni na različitim nivoima apstrakcije. Bezbednosnu argumentaciju treba preispitati kako bi se utvrdile manjkavosti prezentacije dokaza, kao i nedostaci u ispunjenju ciljeva bezbednosne garancije.

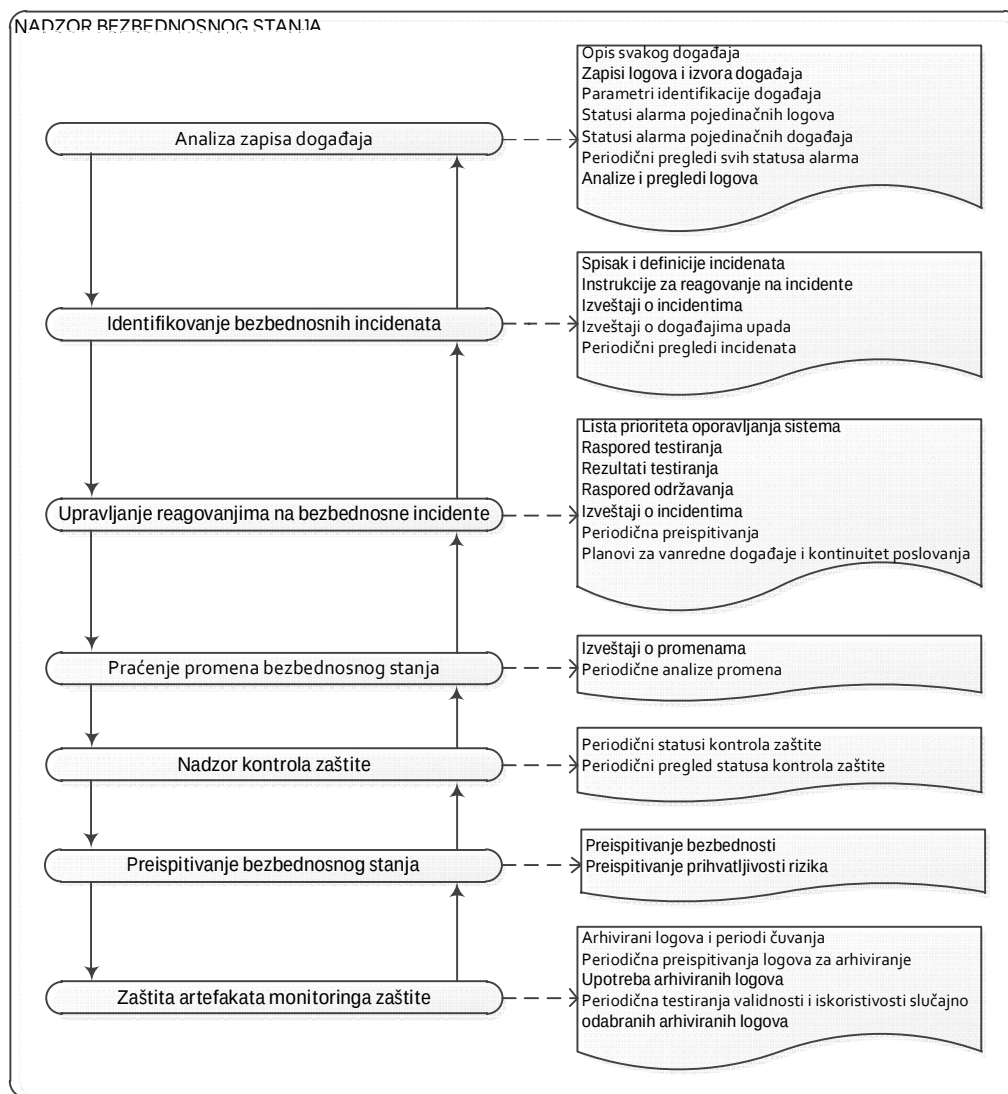
Bezbednosna argumentacija visokog nivoa, može da demonstrira ispunjenje ciljeva relevantnih kriterijuma. Drugi mogući oblik ili deo bezbednosne garancije, može da prikaže način na koji su identifikovane pretnje imovine sistema. Kada je svaki cilj bezbednosne garancije podržan relevantnim i dovoljnim dokazima koji ispunjavaju zahteve primenjivih standarda, takva argumentacija može biti korisna za klijenta, certifikatora zaštite sistema, ili krajnjeg korisnika.

3.2.6 Nadzor bezbednosnog stanja

Proces nadzora bezbednosnog stanja treba da osigura da se sva narušavanja i pokušaji narušavanja bezbednosti, ili greške koje potencijalno mogu izazvati narušavanje bezbednosti, identifikuju i saopšte. Eksterno i interno okruženje mora da se monitoriše, kako bi se uočili svi faktori koji mogu imati uticaj na bezbednost sistema.

Bezbednosno stanje govori o spremnosti sistema i njegovog okruženja da se suoči sa trenutnim pretnjama i ranjivostima, kao i bilo kakvim uticajima na sistem i njegovu imovinu. Ovaj proces uključuje aktivnosti procesa procene ranjivosti i bezbednosnog rizika. Svi podaci prikupljeni iz internog i eksternog okruženja, analiziraju se u sopstvenom kontekstu i u odnosu na ostale podatke o starijim i/ili novijim događajima. Nadzor bezbednosnog stanja odnosi se na okruženje gde se sistem koristi i okruženje u kome je sistem razvijen. Bilo koji pojedinačni sistem treba da funkcioniše u sprezi sa postojećim sistemima koji mogu imati uticaja na celokupnu bezbednost, prema tome, svi postojeći sistemi moraju biti pod nadzorom.

Ovaj proces ima tri cilja: na incidente reagovati u skladu sa politikom; detektovati su i pratiti spoljašnje i unutrašnje bezbednosne događaje; i identifikovati i tretirati promene operativnog stanja bezbednosti u odnosu na bezbednosne ciljeve, što se postiže inženjerskim praksama ilustrovanim na Slika 20 i opisanim u narednom tekstu.



Slika 20 Proces nadzora bezbednosnog stanja

Analiza zapisa događaja

Analiza evidencija događaja utvrđuje njegov uzrok, način odvijanja i verovatnoću ponovne pojave.

Bezbednosno relevantne informacije identifikuju se ispitivanjem istorijskih evidencija i zapisa događaja (kompozicije log zapisa). Događaji od interesa treba da budu identifikovani prema faktorima koji utvrđuju koleraciju određenog događaja iz više različitih zapisa. Tada se višestruki zapisi događaja mogu spojiti u jedan zapis događaja.

Većina kontrolnih tragova (*audit log*) uglavnom sadrže informacije koje se odnose na pojedinačan događaj, što je slučaj u distribuiranom/mrežnom okruženju. Jedan događaj često ostavlja tragove na više različitih lokacija u mreži. Kako bi se osiguralo da svi pojedinačni zapisi budu korisni i da doprinose potpunom razumevanju događaja i njegovog ponašanja, pojedinačni zapisi kontrolnih tragova treba da se kombinuju ili spoje u jedan zapis (evidenciju) događaja.

Analiza može da se vrši nad evidencijama jednog događaja, ili evidencijama o više događaja. Analiza više zapisa istog tipa, često koristi trendove ili statističke tehnike.

Analiza više zapisa različitih tipova može da se izvodi nad zapisima kontrolnih tragova ili zapisima kombinovanih (spojenih) događaja, ali je ipak lakše vršiti analizu zapisa više događaja istog tipa. Alarme, odnosno, zahteve za preduzimanjem akcije na osnovu jednog događaja, treba utvrditi za oba zapisa (kontrolne tragove i spojene događaje). Takođe, u analizu treba uključiti logove i zapise događaja iz razvojnog okruženja.

Tipični rezultati aktivnosti ove inženjerske prakse su:

- Opis svakog događaja – identifikovanje izvora, uticaja i važnosti svakog detektovanog događaja.
- Konstitucija zapisa logova i izvora događaja – zapisi događaja iz raznih izvora.
- Parametri identifikacije događaja – opisuju događaje koji se prikupljaju i ne prikupljaju sa različitih delova sistema.
- Spisak svih trenutnih statusa pojedinačnih kontrolnih tragova alarma – identifikuje sve zahteve za akcijama na osnovu jednog log zapisa.
- Spisak svih trenutnih statusa pojedinačnih događaja alarma – identifikuje sve zahteve za akcijama na osnovu događaja koji su formirani iz više zapisa kontrolnih tragova.
- Periodični izveštaj svih statusa alarma koji su se desili – sintetizacija spiskova alarma iz više sistema, što omogućava da se vrše preliminarne analize.
- Analize i pregledi logova – analiza alarma koji su se nedavno dogodili i izveštaji rezultata za višestruku upotrebu.

Identifikovanje bezbednosnih incidenata

Ova praksa ima za cilj da se utvrdi da li se desio bezbednosno relevantan incident, da se utvrde detalji i, ukoliko je neophodno, podneti izveštj. Bezbednosno relevantni incidenti mogu da se otkriju iz istorijskih podataka o događajima, podataka konfiguracije sistema, rezultata alata za testiranje integriteta i ostalih informacija o sistemu. Pošto se neki incidenti događaju tokom dužeg vremenskog perioda, ova analiza može da sadrži poređenja stanja sistema tokom vremena.

Notes

Bezbednosni incidenti mogu nastati u razvojnem i operativnom okruženju sistema. Ovi incidenti na različite načine mogu uticati na sistem u razvoju ili produkciji. Namerni tehnički napadi hakera ili zlonamernih programa (virusi, crvi, itd.), zahtevaju drugačiji pristup zaštite nego kod slučajnih događaja. Od analize konfiguracije i stanja sistema zahteva se detektovanje napada. Treba pripremiti, testirati i primenjivati odgovarajući plan reagovanja. Mnogi tehnički napadi zahtevaju hitno, unapred definisano reagovanje kako bi se ublažilo ili sprečilo širenje štete. U mnogim slučajevima, nekoordinisani odgovori mogu pogoršati situaciju. Svuda gde je neophodno, treba definisati reagovanje na bezbednosne incidente, kako je to opisano u sledećoj praksi.

Tipični rezultati aktivnosti ove inženjerske prakse su:

- Spisak i definicije incidenata – identifikuje zajedničke bezbednosne incidente i opisuje ih kako bi se lakše prepoznali.
- Instrukcije za reagovanje na incidente – opisuje odgovarajući postupak za reagovanje na incidente koji su se desili.
- Izveštaji o incidentima – sa relevantnim detaljima opisuju koji se incident dogodio, uključujući izvor incidenta, bilo kakvo oštećenje, preduzete akcije i dalje potrebne aktivnosti.

- Izveštaji o svakom detektovanom događaju upada – sa relevantnim detaljima opisuju detektovane pojedinačne događaje upada, uključujući izvor, bilo kakvo oštećenje, preduzete akcije i dalje potrebne aktivnosti.
- Periodični pregledi incidenata – pruža pregled nedavnih incidenata, ističući trendove, oblasti gde je moguća potreba za većom zaštitom, kao i moguće uštede od smanjenja zaštite.

Upravljanje reagovanjima na bezbednosne incidente

U većini slučajeva, od ključne važnosti je održavanje kontinuiteta raspoloživosti sistema. Mnogi događaji se ne mogu sprečiti, pa je sposobnost za reagovanje na bezbednosno relevantne incidente od suštinskog značaja.

Planiranje vanrednih događaja i kontinuiteta poslovanja, zahteva: identifikovanje maksimalno prihvatljivog vremenskog perioda nefunkcionisanja sistema; identifikovanje ključnih elemenata za funkcionisanje sistema; identifikovanje i izradu strategije i plana oporavka; testiranje plana; održavanje plana. U nekim slučajevima vanredne situacije mogu zahtevati reagovanje na incidente i neprijateljske agente (npr. viruse, hakere i sl.).

Ne može se unapred znati koji događaji će se desiti, ali, ako se želi sprečiti kaos, onda njima treba upravljati. Kada situacija prevaziđe unapred identifikovana scenarija, ona se podiže na viši nivo rukovodstvenog odlučivanja.

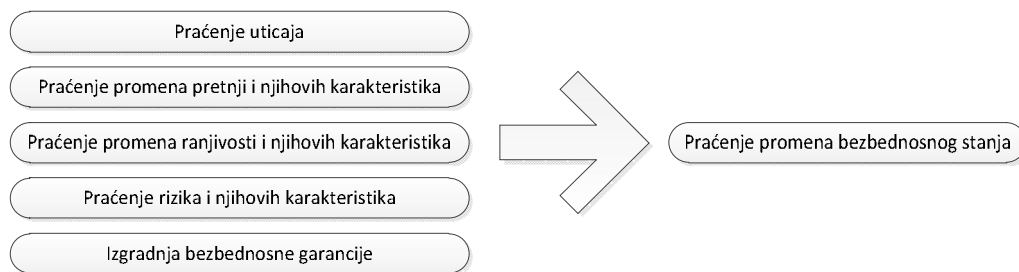
Tipični rezultati aktivnosti ove inženjerske prakse su:

- Lista prioriteta oporavljanja sistema – sadrži opise redosleda kojim će biti očuvane funkcije sistema i oporavljene u slučaju otkaza izazvanog incidentom.
- Raspored testiranja – sadrži datume periodičnog testiranja sistema, kako bi se osiguralo poznavanje i operativnost bezbednosno relevantnih funkcija i procedura.
- Rezultati testiranja – opisuju rezultate periodičnog testiranja i akcije koje treba preduzeti za održanje bezbednosti sistema.
- Raspored održavanja – sadrži datume održavanja sistema, kako preventivnog, tako i nadogradnje (ovaj raspored je uglavnom integrisan sa rasporedom testiranja).
- Izveštaji o incidentima – sa relevantnim detaljima opisuju koji se incident dogodio, uključujući izvor incidenta, bilo kakvo oštećenje, preduzete akcije i dalje potrebne aktivnosti.
- Periodična preispitivanja – opisuju procedure koje treba izvršiti za vreme periodičnih preispitivanja zaštite sistema, uključujući odgovornosti, vrstu provere i rezultata.
- Planovi za vanredne događaje i kontinuitet poslovanja – identifikuju maksimalno prihvatljiv period zastoja sistema, ključne elemente sistema, strateški plan oporavljanja sistema, nastavak poslovanja, upravljanje situacijom i procedure za testiranje i održavanje plana.

Praćenje promena bezbednosnog stanja

Cilj ove prakse je da se otkriju sve promene koje mogu pozitivno i negativno uticati na efektivnost postojećeg bezbednosnog stanja. Zaštita koja se primenjuje u bilo kom sistemu, treba da je u relaciji sa prenjama, ranjivostima, uticajima i rizicima koji se odnose na njegovo interno ili eksterno okruženje. Pretnje, ranjivosti, uticaji i rizici nisu statični i njihove promene utiču na efektivnost i adekvatnost bezbednosnog stanja, zato moraju da se prate i analiziraju njihove promene, kako bi se procenio njihov značaj u pogledu efektivnosti zaštite.

Ova praksa je u tesnoj vezi sa ostalim praksama praćenja promena pretnji, ranjivosti, uticaja, rizika i okruženja, što je ilustrovano na Slika 21.



Slika 21 Bezbednosni ulazi za praćenje promena bezbednosnog stanja

Treba ispitati eksterne i interne izvore promena, kao i izvore promena u razvojnom i produkcionom okruženju. Kada se uoči promena, odmah treba da se pokrene okidač za reagovanje, obično se vrši preispitivanje analize rizika, ili jednog dela analize, koja je uspostavljena u procesu procene bezbednosnog rizika.

Tipični rezultati aktivnosti ove inženjerske prakse su:

- Izveštaji o promenama – identifikuju bilo kakve eksterne i interne promene koje mogu uticati na stanje bezbednosti sistema.
- Periodične provere uticaja promene – analiziranje promena bezbednosnog stanja, kako bi se utvrdio njihov uticaj i potreba za reagovanjem.

Nadzor kontrola zaštite

Nadzor kontrola zaštite uključuje praćenje i ispitivanje promena efektivnosti performansi i funkcionalnosti kontrola zaštite.

Treba redovno nadgledati kontrole zaštite razvojnih i produkcionih okruženja sistema. Većina zaštitnih mera, nakon njihove primene, mogu postati neupotrebljive ili neefektivne. Većina kontrola zaštite prikazuju svoj trenutni status, efektivnost i zahteve za održavanjem. Sva tri aspekta treba periodično preispitivati.

Tipični rezultati aktivnosti ove inženjerske prakse su:

- Periodični status kontrola zaštite – opisuje status postojećih kontrola zaštite u cilju otkrivanja pogrešnih konfiguracija ili ostalih problema.
- Periodični pregled statusa kontrola zaštite – daje pregled stanja postojećih kontrola zaštite, trendova, potreba za poboljšanjem i mogućim uštedama od smanjenja zaštite.

Preispitivanje bezbednosnog stanja

Preispitivati stanja bezbednosti sistema obavlja se radi identifikovanja potrebe za promenama.

Bezbednosno stanje sistema je podložno promenama zbog pretnji iz okruženja, operativnih zahteva i konfiguracije sistema. Ova praksa preispituje razloge primene zaštite i bezbednosne zahteve drugih praksi.

Preispitivanje bezbednosnog stanja treba sprovoditi u trenutnom produkcionom okruženju, ali treba preispitivati i ranije nastale promene. Ukoliko drugi događaji, poput promena, nisu bili deo kompletne provere zaštite, preispitivanje će se nadovezati na poslednje obavljeno preispitivanje, kako bi se ispravili propusti. Periodična preispitivanja treba da se

usaglasene sa zahtevima odgovarajućih politika ili regulativa. Preispitivanja treba da dovedu do ponovne procene adekvatnosti trenutne bezbednosti i nivoa prihvatljivog rizika. Preispitivanje se zasniva na organizacionom pristupu proceni rizika, uspostavljenoj u procesu procene rizika. Razvojno okruženje u kome je kreiran sistem, treba da se preispituje na isti način kao i produkciono okruženje sistema. U stvari, razvojno okruženje može da se posmatra kao operativno (produkciono) okruženje za razvoj sistema.

Tipični rezultati aktivnosti ove inženjerske prakse su:

- Preispitivanje bezbednosti – sadrži opise trenutnog okruženja bezbednosnog rizika i bezbednosnog stanja, kao i analize njihove kompatibilnosti.
- Preispitivanje prihvatljivosti rizika – izjava o prihvatljivosti rizika, da je rizik koji se odnosi na rad sistema prihvatljiv.

Zaštita artefakata monitoringa zaštite

Cilj ove prakse je da se obezbedi adekvatna zaštita artefakata koji se odnose na monitoring zaštite.

Ako rezultati aktivnosti nadzora zaštite nemaju malu vrednost, ova aktivnost podrazumeva zapečaćenje i arhiviranje evidencija monitoringa, izveštaja provere i analize.

Većina aktivnosti nadzora, uključujući proveru, daju određene rezultate. Na ove rezultate može odmah da se reaguje, ili da se snime i sačuvaju za kasniju analizu i upotrebu. Sadržaje evidencija treba dizajnirati tako da pomognu u razumevanju incidentnog događaja i da prikažu promene u trendovima. Evidencijama treba upravljati u skladu sa politikom organizacije i zakonskim regulativama. Evidencije moraju biti pouzdane i zaštićene od slučajnog ili namernog ošteđenja. Kada se dnevnik evidencija napuni, treba koristiti novi, ili ga preispitati i arhivirati, ili zameniti sa praznim. Kada se evidencije redefinišu, sve zapise koji nisu neophodni (koji se ne zahtevaju) treba ukloniti i primeniti druge načine redukovanja veličine i količine zapisa. Kako bi se sprečile bilo kakve nekontrolisane izmene, zapise treba zapečatiti i arhivirati u propisanom periodu.

Tipični rezultati aktivnosti ove inženjerske prakse su:

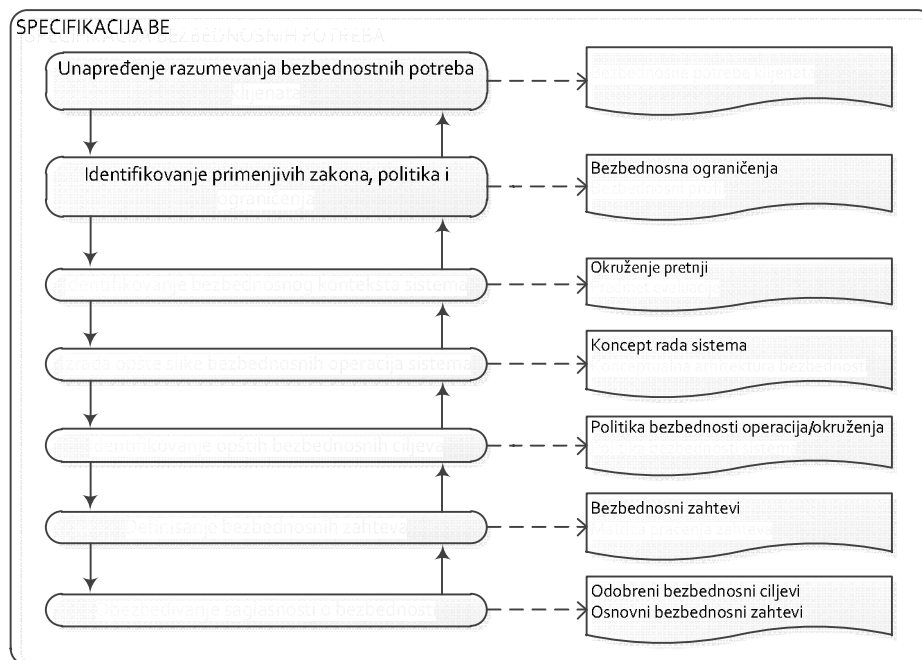
- Spisak svih arhiviranih logova sa periodom čuvanja – identifikuje gde se artefakti monitoringa čuvaju i kada se uništavaju.
- Periodični rezultati preispitivanja logova koje treba arhivirati – opis svakog nedostajućeg izveštaja i identifikacija odgovarajućeg odgovora.
- Upotreba arhiviranih logova – identifikuje korisnike arhiviranih logova, uključujući vreme i razlog pristupa, uz dodatne komentare.
- Periodični rezultati testiranja validnosti i iskoristivosti slučajno odabranih arhiviranih logova – analiza slučajno odabranih logova i utvrđivanje njihove kompletnosti, ispravnosti i korisnosti, u cilju osiguranja adekvatnosti monitoringa zaštite sistema.

3.2.7 Specifikacija bezbednosnih potreba

Specifikacija bezbednosnih potreba služi da se eksplicitno identifikuju potrebe koje se odnose na bezbednost sistema, gde se vrši definisanje osnovne konfiguracije zaštite sistema kako bi se zadovoljili svi zakonski i organizacioni bezbednosni zahtevi, kao i zahtevi politike bezbednosti. Ove potrebe su prilagođene kontekstu operativnih ciljeva zaštite sistema, postojećem okruženju zaštite sistema i skupu identifikovanih bezbednosnih ciljeva. Usvajanje osnovne konfiguracije zaštite sistema proverava se ispunjenjem definisanog skupa bezbednosnih zahteva za sistem.

Ovaj proces obuhvata aktivnosti koje definišu sve aspekte zaštite u celokupnom informacionom sistemu, uključujući fizičku, funkcionalnu i proceduralnu zaštitu. Njegove bazične prakse opisuju načine identifikovanja bezbednosnih potreba i njihovu prerađu u koherentne bezbednosne zahteve za osnovnom konfiguracijom zaštite, koja se koristi u dizajnu, razvoju, verifikaciji, operativnom radu i održavanju sistema. U većini slučajeva potrebno je uzeti u obzir postojeće okruženje i njegove bezbednosne potrebe. Kako bi se osiguralo ispunjenje bezbednosnih potreba klijenata, izlazne informacije ovog procesa se prikupljaju i dalje prerađuju, koriste i ažuriraju u toku životnog veka projekta, što se vrši u procesu obezbeđivanja bezbednosnog ulaza.

Osnovni cilj ove prakse je da se, među svim stranama uključenim u poslovni proces, uključujući i klijente, postigne opšte razumevanje bezbednosnih potreba. Ovi ciljevi se postižu inženjerskim praksama ilustrovanim na Slika 22 i opisanim u narednom tekstu.



Slika 22 Proces specifikacije bezbednosnih potreba

Unapređenje razumevanja bezbednosnih potreba klijenata

Ovde se vrši prikupljanje informacija potrebnih za opšte razumevanje bezbednosnih potreba klijenata. Ove potrebe su pod uticajem veličine i značaja bezbednosnog rizika za klijenta, kao i okruženja u kom će se sistem koristiti.

Pojam „klijent“ može da se odnosi na određenog naručioca proizvoda, sistema ili usluge, a može da se odnosi generalno na korisnike određene ciljne grupe, zasnovane na markentiškom istraživanju. Po nekad je potrebno identifikovati i razlikovati različite grupe korisnika. Na primer, obični korisnici mogu imati drugačije potrebe od administratora.

Na kraju, kreira se izjava o bezbednosnim potrebama klijenata, koja sadrži generalni opis bezbednosnih zahteva klijenata.

Identifikovanje primenjivih zakona, politika i ograničenja

U ovoj praksi se vrši identifikovanje zakona, politika, standarda, eksternih uticaja i ograničenja sistema.

Namena ove prakse je da se prikupe svi eksterni faktori koji imaju uticaj na bezbednost sistema. Određivanje njihove primenjivosti kreće od identifikovanja zakona, regulativa, politika i komercijalnih standarda koji diktiraju rad predmetnog okruženja sistema. Pored toga, treba odrediti prioritete među globalnim i lokalnim politikama. Treba postaviti systemske bezbednosne zahteve klijenta i identifikovati i izdvojiti bezbednosne uticaje.

Posebnu pažnju treba obratiti na sistem koji proteže na više fizičkih oblasti. Konflikt se može pojaviti između zakona i regulativa koji nisu primenjivi u različitim državama ili tipovima poslovanja. Zato, u procesu identifikovanja bezbednosnih uticaja, konflikte treba svesti na minimum, ili ih eliminisati. Tipični rezultati ovih aktivnosti su:

- Bezbednosna ograničenja – zakoni, politike, regulative i ostala ograničenja koja utiču na bezbednost sistema.
- Bezbednosni profil – bezbednosno okruženje (pretnje, politike organizacije); bezbednosni ciljevi (npr. pretnje kojima se treba suprotstaviti); zahtevi bezbednosne funkcionalnosti i garancije; argumentacija da će sistem koji je razvijen prema tim zahtevima ispuniti ciljeve.

Identifikovanje bezbednosnog konteksta sistema

Kontekst zaštite sistema se određuje na osnovu namene sistema. Ova praksa treba da identifikuje kako kontekst sistema utiče na bezbednost. Prvo treba razumeti namenu sistema (npr. obaveštajni rad, finansije, zdravstvo). Potom se procenjuje bezbednosni značaj scenarija operativnih zadataka, a u toj fazi se zahteva opšte razumevanje pretnji kojima sistem može biti izložen. Procenjuju se mogući uticaji funkcionalnih zahteva i zahteva za performansama sistema. Takođe, preispituju se bezbednosni uticaji operativnih ograničenja.

Prilikom definisanja granica zaštite okruženja, treba uzeti u obzir da okruženje podrazumeva i interfejs sa drugim organizacijama ili sistemima. Elementi interfejsa se određuju da budu unutar ili izvan granica zaštite okruženja.

Različiti eksterni faktori utiču različitim stepenom bezbednosnih potreba organizacije. Ovi faktori uključuju političku orijentaciju i promene u političkom fokusu, tehnološki razvoj, ekonomske uticaje, globalna dešavanja i aktivnosti informacionog ratovanja. Pošto nijedan od ovih faktora nije statički, oni zahtevaju praćenje promena i periodičnu procenu potencijalnih bezbednosnih uticaja na sistem.

Granice zaštite sistema nisu obavezno identične granicama sistema. Na primer, granice zaštite mogu da obuhvataju objekte gde se nalazi sistem i osoblje koje koristi sistem, dok granice sistema mogu da dosegnu do interfejsa mašine sa čovekom. Zbog ovakvog koncepta proširenja granica zaštite, kontrole fizičke zaštite se posmatraju kao efektivnije mere kontrole pristupa od čisto tehničkih mera.

Tipični rezultati ove inženjerske prakse su:

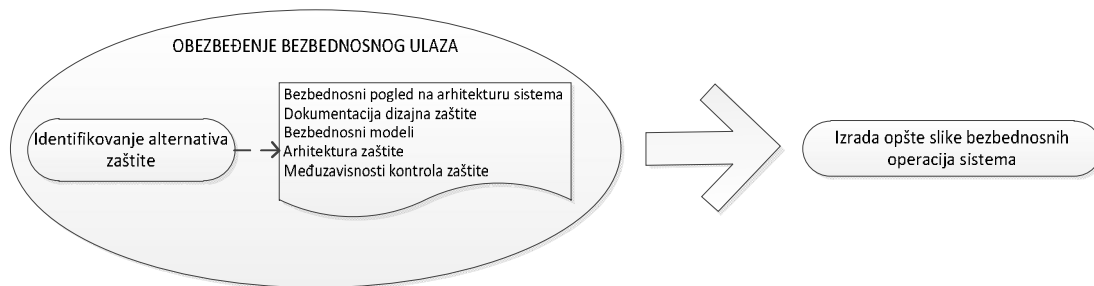
- Očekivano okruženje pretnji – svaka poznata ili pretpostavljena pretnja sistemu, od koje se treba zaštititi; uključujući agente pretnji (stručnost, raspoloživi resursi, motivacija), napade (metodi, ranjivosti izloženosti, prilika) i vrednost/atraktivnost imovine.
- Predmet evaluacije – opis sistema, ili proizvoda, čije bezbednosne karakteristike treba evaluirati (tip, namena, opšte karakteristike, ograničenja u korišćenju).

Izrada opšte slike bezbednosnih operacija sistema

Cilj ove prakse je da se kreira opšta bezbednosna slika rada sistema.

Ova praksa definiše visoki nivo pogleda na zaštitu preduzeća, uključujući uloge, odgovornosti, tokove informacija, imovinu, resurse, zaštitu персонала i fizičku zaštitu. Ovaj opis treba da sadrži diskusiju o tome, kako preduzeće može da se vodi u okviru ograničenja sistemskih zahteva. Ovaj pogled na sistem je tipično bezbednosni koncept operacija i treba da sadrži najširi pregled bezbednosne arhitekture sistema, procedura i okruženja. Takođe, u ovoj fazi, pored operativnog okruženja, treba obuhvatiti zahteve koji se odnose na razvojno okruženje sistema. Na kraju, izrađuju se dve vrste dijagrama bezbednosne arhitekture:

- Bezbednosni koncept sistemskih operacija – Visoki nivo pogleda na bezbednost sistema (uloge, odgovornosti, imovina, tokovi informacija, procedure).
- Konceptualna arhitektura bezbednosti – Konceptualni pogled na bezbednosnu arhitekturu. Kao bezbednosni ulaz za dobijanje ove arhitekture, koriste se rezultati prakse identifikovanja bezbednosnih alternativa, procesa obezbeđivanja bezbednosnog ulaza, što je ilustrovano na Slika 23.

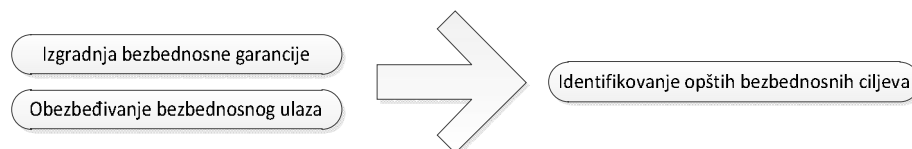


Slika 23 Bezbednosni ulazi za izradu konceptualne arhitekture bezbednosti sistema

Identifikovanje opštih bezbednosnih ciljeva

Aktivnosti ove prakse usmerene su na identifikovanje bezbednosnih ciljeva, koji zahtevaju da se obezbedi adekvatna bezbednost operativnog okruženja sistema. Na ove ciljeve mogu uticati ciljevi bezbednosne garancije sistema, utvrđeni u procesu izgradnje bezbednosne garancije.

Ciljevi treba da budu, koliko god je to moguće, nezavisni od bilo koje pojedinačne implementacije. Ukoliko su u posmatranom okruženju prisutna određena ograničenja, ona treba da budu utvrđena u procesu obezbeđivanja bezbednosnog ulaza, gde se utvrđuju informacije o bezbednosnim ograničenjima koje se koriste u inženjerskim aktivnostima, što je prikazano na Slika 24. Bezbednosni ciljevi, minimalno treba da su usmereni na zahteve raspoloživosti, kontrolisane odgovornosti, autentičnosti, poverljivosti, integriteta i pouzdanosti sistema i informacija.



Slika 24 Bezbednosni ulazi za identifikovanje opštih bezbednosnih ciljeva

Tipični rezultati ove inženjerske prakse su:

- Politika bezbednosti operacija/okruženja – pravila, direktive i prakse koje regulišu način upravljanja, zaštite i distribucije imovine, unutar i van organizacije.
- Politika bezbednosti sistema – pravila, direktive i prakse koje regulišu način upravljanja, zaštite i distribucije imovine sistema ili proizvoda.

Definisanje bezbednosnih zahteva

Ova praksa služi za definisanje konzistentnog skupa bezbednosnih zahteva sistema, koji se odnose na zaštitu koju treba implementirati u sistemu. Praksa treba da obezbedi, da svaki zahtev bude konzistentan sa primenjivom politikom, zakonima, standardima, čiji zahtevi utiču na sistem.

Bezbednosni zahtevi treba potpuno da definišu bezbednosne potrebe sistema, uključujući i one zahteve koji se mogu ispuniti netehničkim sredstvima. Obično je potrebno definisati ili odrediti granice posmatranog dela sistema, logičke ili fizičke, kako bi se osiguralo da su obuhvaćeni svi bezbednosni aspekti. Bezbednosne zahteve treba mapirati, ili staviti u odnos sa sistemskim ciljevima, kako bi bili jasni, koncizni i da međusobno nisu kontradiktorni. Kad god je moguće, treba minimizirati uticaje zaštite na funkcionalnost i performanse sistema. Bezbednosni zahtevi treba da obezbede osnovu za evaluaciju bezbednosti sistema u posmatranom okruženju.

Mnogi zahtevi se odnose na više disciplina, tako da ima samo nekoliko isključivo bezbednosnih zahteva. Prema tome, ova oblast procesa zahteva da se radi uz veliku koordinaciju sa drugim disciplinama, što daje rezultate tačno onakve kakvi se zahtevaju od sistema. Aktivnosti ovakvih interakcija opisani su u procesu bezbednosne koordinacije.

Tipični rezultati ove inženjerske prakse su:

- Bezbednosni zahtevi – zahtevi koji imaju direktan uticaj na bezbedan rad sistema, ili zahtevaju usklađenost sa zahtevima određene politike zaštite.
- Matrica praćenja zahteva – mapiranje bezbednosnih potreba sa zahtevima za rešenjima (npr. arhitektura, dizajn, implementacija), testiranjem i rezultatima testiranja.

Obezbeđivanje saglasnosti o bezbednosti

Cilj ove prakse je da se od svih relevantnih strana dobije saglasnost o bezbednosnim zahtevima, odnosno, da se definiše ugovor o bezbednosnim zahtevima koji se podudaraju sa potrebama klijenta.

U slučajevima gde postoje generičke grupe, a ne određeni klijent, zahtevi treba da zadovolje skup zadatah ciljeva. Takvi bezbednosni zahtevi moraju biti potpuni i da odražavaju opšte politike, zakone i korisničke potrebe. Pre dobijanja saglasnosti, potrebno je identifikovati i ponovo obraditi sve uočene nedostatke u zahtevima.

Najvažnije je osigurati da ono što je dogovoreno, svima bude podjednako razumljivo. Naročito je potrebno obezbediti, da bezbednosni zahtevi imaju isto značenje svima koji su uključeni u proces. Rezultati ovih aktivnosti su:

- Odobreni bezbednosni ciljevi – Potvrđene izjave o nameri da se organizacija suoči sa pretnjama i/ili usaglasila sa identifikovanim politikama bezbednosti.
- Osnovni bezbednosni zahtevi – Minimalan skup bezbednosnih zahteva koji su dogovoreni među svim stranama (naročito sa korisnikom), za sve utvrđene ključne tačke projekta.

3.2.8 Obezbeđivanje bezbednosnog ulaza

Ovaj proces takođe zasluđuje da se ukratko opiše, jer je uključen u sve inženjerske aktivnosti, tako što ih snadbeva informacija koje su neophodne za bezbedan razvoj i upotrebu sistema.

Namena ovog procesa je da arhitektama sistema, dizajnerima i imolemtatorima, ili korisnicima, obezbedi neophodne bezbednosne informacije. Ove informacije sadrže alternative i uputstva za arhitekturu ili implementaciju zaštite. Razvoj i analiza bezbednosnih ulaza koordinirano obavljaju relevantni članovi organizacije, na osnovu bezbednosnih potreba identifikovanih u gore opisanom procesu specifikacije bezbednosnih potreba.

Bezbednosni ulazi koje obezbeđuje ovaj proces, služe kao podrška aktivnostima dizajniranja i implementacije sistema. Proces se fokusira na bezbednost, kao integralni deo sistema. Njegove bazične prakse koriste ulaze iz inženjerskih procesa cele organizacije i obezbeđuju specifične bezbednosne rezultate, koje zatim vraćaju svim inženjerskim procesima. Identifikovani inženjerski procesi odnose se na razvoj novih objekata i operacija, ili na održavanje postojećih.

Obezbeđivanje bezbednosnog ulaza obuhvata razvoj (dizajnere i implementatore) i operacije (korisnike i administratore). Kombinovanjem bezbednosnih aktivnosti dizajna i implementacije u jednu oblast procesa naglašava se da su te aktivnosti veoma slične, ali su na različitim nivoima apstrakcije. Alternativna rešenja se kreću u opsegu od celokupne arhitekture sistema, do pojedinačnih komponentata sistema. Neki aspekti bezbednosnih zahteva, pored samog sistema, odnose se i na uticaje okruženja u kome se sistem razvija.

Sve bazične prakse u okviru ove oblasti procesa mogu biti iterativne, pa se može očekivati da se pojave u više tačaka životnog ciklusa razvoja sistema. One su usmerene na ispunjenje tri osnovna cilja:

- Sva sistemska sporna pitanja treba da budu preispitana na bezbednosne uticaje i rešena u skladu sa bezbednosnim ciljevima.
- Svi članovi projektnog tima treba da imaju razumevanje o bezbednosti i da primenjuju bezbednosne ulaze (uputstva i instrukcije) u obavljanju svojih funkcija.
- Sistemska rešenja treba da odražavaju obezbeđene bezbednosne ulaze.

4 ZAKLJUČAK

U suštini, metrike zaštite informacija su prosta interpretacija podataka. Koncepti merenja i metrike su jasni, imaju podršku specijalista zaštite i veliku vrednost za organizaciju. Svi rukovodioci smatraju da bez merenja nema ni upravljanja. Kako promene na tržištu utiču na poslovanje, tako i promene poslovanja utiču na upravljanje zaštitom informacija. Da bi metrike zaštite bile od koristi poslovdstvu, aktivnosti zaštite moraju da prate promene poslovnih aktivnosti, pa će podaci za izradu metrike zaštite uvek biti aktuelni i objektivni.

Najbolji način razvoja programa metrike zaštite informacija je da se u prvoj iteraciji odradi ono što je lakše i jeftinije, što najbrže daje rezultate i da se maksimalno koriste postojeća merenja i metrike. Uvek treba imati na umu da svaka metrika zaštite služi za poboljšanje procesa zaštite i da njen značaj za organizaciju mora da bude jasno prezentovan i potkrepljen činjenicama. Ako se za prezentovanje rezultata metrike zaštite koriste komparativne tabele rezultata, biće zadovoljeni zahtevi svih zainteresovanih strana, jer su aktivnosti zaštite direktno postavljeni u odnos sa poslovnim aktivnostima preduzeća.

Na osnovu ključnih rezultata istraživanja primene metrika zaštite u praksi omogućena je praktična polazna osnova za izradu programa metrike zaštite, iz koje se mogu izvući korisne preporuke koje obavezno treba uzeti u obzir:

- *Da bi se razvio najpogodniji način prezentacije, pre izbora metrike i prikupljanja podataka za metriku, treba poznavati aktuelne poslovne tokove u organizaciji.*
- *Istraživanje i diskutovanje o stvarnim potrebama zainteresovanih strana (npr. sa poslovdstvom, izvršnim rukovodstvom i osobljem za zaštitu informacija).*
- *Odrediti nivo detalja u metodologiji prikupljanja podataka (npr. veoma detaljna ili opšta).*
- *Program metrike zaštite se gradi postepeno i sa opštim informacijama.*
- *Izraditi koncept programa metrike zaštite i pre njegove primene obavezno se konsultovati sa relevantnim učesnicima.*
- *Pre svega, osigurati da metrika zaštite odgovara osoblju za zaštitu informacija.*
- *Oblast primene treba suziti (ne treba odjednom prikupljati mnogo podataka).*
- *Fokusirati se na male oblasti (ne treba krenuti sa sveobuhvatnom metrikom, koncept metrike prvo treba primeniti na jednoj lokaciji ili organizacionoj celini).*
- *Metriku prvo testirati sa osobljem za zaštitu informacija.*
- *Redovno preispitivati odabranu metriku.*
- *Metriku treba što pre promeniti ako ne daje korisne informacije.*

Troškovi pripreme, prikupljanja i prezentacije metrike zaštite, takođe mogu biti predmet diskusije sa relevantnim učesnicima. Pošto je implementacija metrike zaštite program tekuće prirode, a ne projekat, moguće je planirati fondove i za naredne godine.

Ne treba očekivati ili obećavati brze rezultate programa metrike zaštite. Može proći izvesno vreme dok se ne shvati koje podatke treba prikupljati i koji će rezultati metrike biti indikativni i korisni za donošenje poslovnih odluka. Ukoliko se detaljno krene sa odabranom metrikom, a ona ne ispunji postavljene ciljeve, biće potrebno mnogo više vremena za izbor nove metrike i ocenu njene primenljivosti, što nije dobro, jer dinamika poslovanja ne trpi uzaludno potrošeno vreme i izgovore da je trebalo izabrati drugu metriku zaštite.

Faktori koji omogućavaju da program merenja zaštite informacija doprinese kontinualnom poboljšanju sistema zaštite informacija su sledeći:

- Posvećenost rukovodstva i obezbeđenje odgovarajućih resursa;
- Postojanje procesa i procedura zaštite informacija;
- Ponovljivi procesi prikupljanja i izveštavanja korisnih podataka koji obezbeđuju relevantne trendove za određene vremenske periode;
- Kvantitativna merenja bazirana na ciljevima zaštite informacija;
- Podaci koji se lako prikupljaju i koriste u merenjima;
- Evaluacija efektivnosti programa merenja zaštite informacija i implementacija identifikovanih unapređenja;
- Konzistentno periodično prikupljanje, analiza i izveštavanje podataka merenja prema njihovom značaju;
- Korišćenje rezultata merenja od strane relevantnih zainteresovanih strana kako bi identifikovali potrebu za unapređenjem programa zaštite informacija;
- Prihvatanje povratnih informacija od relevantnih zainteresovanih strana; i
- Evaluacija iskoristivosti rezultata merenja i implementacija identifikovanih unapređenja.

Nakon uspešne implementacije programa merenja performansi zaštite informacija, može se:

- Demonstrirati usklađenost organizacije sa primenjivim regulativama, zakonskim i ugovornim zahtevima;
- Doprineti identifikovanju izostavljenih ili nepoznatih bezbednosnih problema;
- Rukovodstvu predstaviti merenje hronoloških i trenutnih aktivnosti zaštite; i
- Obezbediti ulaz u proces upravljanja bezbednosnim rizicima, interne provere i preispitivanje programa zaštite informacija.

PRILOG A. PRIMERI MERENJA ZAŠTITE INFORMACIJA (NIST)

Odvajanje vremena za uspostavljanje merenja performansi zaštite informacija je od ključne važnosti za izvlačenje maksimalne vrednosti iz merenja performansi zaštite informacija.

U ovom prilogu su ponuđeni primeri merenja na programskom i sistemskom nivou. Primeri merenja uključaju programska merenja zaštite informacija i merenja koja odgovaraju minimalnim bezbednosnim zahtevima Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, koji uključuju 17 familija kontrola zaštite iz NIST SP 800-53. Ovi primeri nisu namenjeni za kompletno usvajanje, ali organizacije ih mogu iskoristiti ili adaptirati za merenje performansi svog programa zaštite informacija. Primeri izrade uključuju specifične vremenske okvire, dokaze implementacije, izvore podataka, formule, formate izveštavanja, frekvenciju, odgovorne strane i dopušta dodavanje dodatnih polja na šablon. Treba napomenuti da ova merenja nisu kompletna za ispunjenje minimuma zahteva zaštite informacija iz FIPS 200, ali mogu uputiti na jedan ili više aspekata zahteva. Organizacije moraju da razviju dodatna merenja koja će zadovoljiti njihove potrebe.

Ovi primeri merenja su specifični za implementirane kontrole zaštite na programskom ili sistemskom nivou i uključuju sve tipove merenja – implementaciju, efektivnost/efektivnost i uticaj.

Identification and Authentication (IA) (system-level)

Measure ID	User Accounts Measure 1 (or a unique identifier to be filled out by the organization)
Goal	• <i>Strategic Goal:</i> Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. • <i>Information Security Goal:</i> All system users are identified and authenticated in accordance with information security policy.
Measure	Percentage (%) of users with access to shared accounts NIST SP 800-53 Controls - AC-2: Account Management, AC-3: Access Enforcement, and IA-2: User Identification and Authentication
Measure Type	Effectiveness/Efficiency
Formula	(Number of users with access to shared accounts/total number of users) * 100
Target	This should be a low percentage defined by the organization.
Implementation	1. How many users have access to the system (IA-2)?
Evidence	2. How many users have access to shared accounts (AC-2)?
Frequency	Collection Frequency: Organization-defined (example: monthly) Reporting Frequency: Organization-defined (example: monthly)
Responsible Parties	• Information Owner: Organization-defined (example: System Owner, System Administrator) • Information Collector: Organization-defined (example: System Administrator) • Information Customer: Chief Information Officer (CIO), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])
Data Source	Configuration Management Database, Access Control List, System-Produced User ID Lists
Reporting Format	Pie chart comparing the percentage of users with access to shared accounts versus the percentage of users without access to shared accounts

Incident Response (IR) (program-level and system-level)

Measure ID	Incident Response Measure 1 (or a unique identifier to be filled out by the organization)
------------	---

Goal	• <i>Strategic Goal: Make accurate, timely information on the organization's programs and services readily available.</i> • <i>Information Security Goal: Track, document, and report incidents to appropriate organizational officials and/or authorities.</i>
Measure	Percentage (%) of incidents reported within required time frame per applicable incident category (the measure will be computed for each incident category described in Implementation Evidence) NIST SP 800-53 Controls - IR-6: Incident Reporting
Measure Type	Effectiveness/Efficiency
Formula	For each incident category (number of incidents reported on time/total number of reported incidents) *100
Target	This should be a high percentage defined by the organization.
Implementation Evidence	1. How many incidents were reported during the period (IR-6)? Category 1 - Unauthorized Access? Category 2 - Denial of Service? Category 3 - Malicious Code? Category 4 - Improper Usage? Category 5 - Scans/Probes/Attempted Access? Category 6 - Investigation? 2. How many incidents involving personally identifiable information (PII) were reported during the period (IR-6)? 3. Of the incidents reported, how many were reported within the prescribed time frame for their category, according to the time frames established by US-CERT (IR-6)? Category 1 - Unauthorized Access? Category 2 - Denial of Service? Category 3 - Malicious Code? Category 4 - Improper Usage? Category 5 - Scans/Probes/Attempted Access? Category 6 - Investigation? 4. Of the PII incidents reported, how many were reported within the prescribed time frame for their category, according to the time frames established by US-CERT and/or OMB Memorandum(s) (IR-6)?
Frequency	Collection Frequency: Organization-defined (example: monthly) Reporting Frequency: Organization-defined (example: annually)
Responsible Parties	• Information Owner: Organization-defined (example: Computer Security Incident Response Team [CSIRT]) • Information Collector: Organization-defined (example: System Owner, Information Security Officer [ISSO], CSIRT) • Information Customer: Chief Information Officer (CIO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])
Data Source	Data Source Incident logs, incident tracking database (if available)
Reporting Format	For one-time snapshot - stacked bar chart illustrating the proportion of reported incidents per category that were reported on time For trends - line chart where each line represents an individual category plus a line representing 100 percent

PRILOG B. PRIMERI MERENJA ZAŠTITE INFORMACIJA (ISO27k)

Forum za upravljanje sistemima zaštite informacija ([ISO27k Forum](#)) preporučuje merenja svih 39 ciljeva kontrole standarda ISO/IEC 27002, čemu su doprineli članovi foruma.

Većina merenja zaštite informacija su u originalu preuzete iz radionice [ISACA in Wellington, New Zealand](#) i naknadno ažurirane novim idejama iz [presentation/tutorial by Dan Geer](#), [book by Andrew Jaquith](#) i nastavljena od strane [Gary Hinson](#).

Title/name of metric	Code complexity	
Primary customer	CIO	
Information source/s	McCabe Cyclomatic statistics from development environments	
How calculated	1 / McCabe cyclomatic figure	
Frequency	Once per developed system	
Rationale for measuring this	Complexity is the enemy of security, so reducing complexity (to increase this metric) is a worthwhile security goal	
Relevant section/s of ISO/IEC 27002 Main <i>Subsidiary</i>	4. Risk mgmt 5. Security policy 6. Information security governance 7. Asset mgmt 8. HR 9. Physical security	10. Comms/Ops mgmt 11. Access control 12. SDCL 13. Incident mgmt 14. Continuity mgmt 15. Compliance
Karakteristike merenja	Leading / Lagging / Semi Soft / Hard / Semi	Objective / Subjective / Semi Absolute / Relative (trend) / Semi Confidentiality / Integrity / Availability
Alternative metrics considered	1 / lines of code squared (a less sophisticated measure of code complexity)	
Notes		

PRILOG C. PRIMER KONSTRUKCIJE MERENJA (ISO/IEC)

Information Security Awareness Compliance

Measurement Construct Identification	
Measurement Construct Name	Information security awareness policy compliance
Numerical Identifier	Organization-specific.
Purpose of Measurement Construct	Assess status of compliance with organization security awareness policy among relevant personnel
Control/process Objective	A.8.2 During employment Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.
Control (1)/process (1)	A.8.2.2 All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. (Implementation) All personnel relevant to the ISMS must receive information security awareness training before being granted access to an information system. The training includes
Control (2)/process (2)	A.8.2.1 Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization. (Implementation) All personnel relevant to the ISMS must sign user agreements before being granted access to an information system.
Object of Measurement and Attributes	
Object of Measurement	1.1. Information security awareness training plan/schedule 1.2. Personnel who have completed or in progress in the training. 2.1. Plan for signing user agreements/schedule 2.2. Personnel having signed agreements
Attribute	1.1. Personnel identified in plan 1.2. Personnel status with regard to the training 2.1. Personnel identified in plan for signing 2.2. Personnel status with regard to the signing of agreements
Base Measure Specification	
Base Measure	1.1. Number of personnel planned to date 1.2. Number of personnel who signed 2.1. Number of personnel planned for signing to date 2.2. Number of personnel having signed to date
Measurement Method	1.1. Count number of personnel scheduled to have signed and completed the training to date 1.2. Ask responsible individual for percent of personnel who have completed the training and signed. 2.1. Count number of personnel scheduled to have signed by this date 2.2. Count number of personnel having signed user agreements
Type of Measurement Method	1.1. Objective 1.2. Subjective 2.1. Objective 2.2. Objective
Scale	1.1. Integers from zero to infinity 1.2. Integers from zero to one hundred 2.1. Integers from zero to infinity 2.2. Integers from zero to infinity
Scale type	1.1. Ordinal 1.2. Ratio 2.1. Ordinal 2.2. Ordinal

Unit of Measurement	1.1. Personnel 1.2. Percentage 2.1. Personnel 2.2. Personnel
Derived Measure Specification	
Derived Measure	1. Progress to date 2. Progress to date with signing
Measurement Function	1. Add status for all personnel having signed, planned to be completed to date 2. Divide Personnel having signed to date by Personnel planned for signing to date
Indicator Specification	
Indicator	a) Status expressed as a combination of ratios and; b) Trend
Analytical Model	a) [Divide Progress to Date by (Personnel Planned to Date times 100)] and Progress to date with signing b) Compare Status with Previous Statuses'
Decision Criteria Specification	
Decision Criteria	a) Resulting ratios should fall respectively between 0.9 and 1.1 and between 0.99 and 1.01 to conclude the achievement of the control objective and no action; and; b) Trend should be upward or stable.
Measurement Results	
Indicator Interpretation	Interpretation for the indicator a) should be as follows: - The organization criteria for compliance with organization security awareness policy have been met satisfactorily at $0.9 < 1st\ ratio < 1.1$ and $0.99 < 2nd\ ratio < 1.01$; corresponding to standard font; - The organization criteria have been met unsatisfactorily at $[1st\ ratio < 0.9\ or\ 1st\ ratio > 1.1]$ and $0.99 < 2nd\ ratio < 1.01$; corresponding to italic; - The organization criteria are not met at $[2nd\ ratio < 0.99\ or\ 2nd\ ratio > 1.01]$; corresponding to bold. Interpretation for the indicator b) should be as follows: - Upward trend indicates improved compliance, downward trend indicates deteriorating compliance. The degree of trend change may provide insights into the effectiveness of control implementation. Sharp changes in either direction indicate that control implementation requires close examination to determine the cause. Negative trends may require management intervention. Positive trends should be examined to identify potential best practices.
Reporting Formats	Standard Font = Criteria have been met satisfactorily Italic Font = Criteria have been met unsatisfactorily Bold Font = Criteria have not been met
Stakeholders	
Client for measurement	Managers responsible for an ISMS. Security Management. Training Management.
Reviewer for measurement	Security Manager.
Information Owner	Information Security Officer and Training Manager.
Information Collector	Training Management - Human Resource Department.
Information Communicator	Managers responsible for an ISMS.
Frequency/Period	
Frequency of Data Collection	Monthly, first working day of the month.
Frequency of Data Analysis	Quarterly.
Frequency of Reporting Measurement Results	Quarterly.
Measurement Revision	Review annually
Period of Measurement	Annual

PRILOG D. FUNKCIONALNA I INFORMACIONA IMOVINA SISTEMA

Pre procene vrednosti imovine potrebno je identifikovati imovinu (sa odgovarajućim nivoom detalja). Međunarodni standard ISO/IEC 27005:2008 razlikuje dve vrste imovine:

1. Primarna imovina
 1. Poslovni procesi i aktivnosti
 2. Informacije
2. Svi tipovi sredstava za podršku (na koje se oslanja primarna imovina)
 1. Hardver
 2. Softver
 3. Mreža
 4. Personal
 5. Lokacija
 6. Organizaciona struktura

D-1 PRIMARNA IMOVINA

Identifikovanjem primarne imovine postaje mnogo jasnije područje primene zaštite. Ova identifikacija se vrši u radnoj grupi sastavljenoj od predstavnika procesa (menadžeri, IT specijalisti i korisnici).

Primarnu imovinu uglavnom čine glavni procesi i informacije koje se koriste u aktivnostima procesa. Ostali procesi takođe mogu da se uključe, kako bi se lakše izradila politika bezbednosti ili plan kontinuiteta poslovanja. U zavisnosti od namene, negde neće biti potrebna detaljna analiza svih elemenata područja primene zaštite. U ovakvim slučajevima, analiza može da se ograniči na ključne elemente. Postoje dva tipa primarne imovine:

D-1.1 Poslovni procesi/podproces i aktivnosti

- Proces i čiji zastoj ili degradacija čini misiju organizacije nemogućom.
- Proces koji sadrži tajne procese ili vlasničku tehnologiju (veoma vredna lična imovina, može biti zakonski zaštićena).
- Proces koji, ako se modifikuju, mogu uveliko uticati na ispunjenje misije organizacije.
- Proces koji su neophodni da bi organizacija ispunila ugovorne ili zakonske obaveze.

D-1.2 Primarne informacije

- Vitalne informacije za ostvarenje misije organizacije ili poslovnih ciljeva.
- Lične informacije, kako su zakonski definisane.
- Strateške informacije, koje su potrebne za ostvarenje strateških ciljeva.
- Skupe informacije, čije prikupljanje, skladištenje, obrada i prenos zahteva mnogo vremena i/ili visoke troškove prikupljanja.

Procesi i informacije koji u ovoj analizi nisu identifikovani kao osetljivi, neće biti klasifikovani. Što znači, čak i ako proces ili informacija budu kompromitovani, organizacija će i dalje biti u stanju da uspešno ostvari svoju misiju. Ali, one informacije i procesi koji su identifikovani kao osetljivi, naslediće implementirane kontrole zaštite procesa i informacija.

D-2 SREDSTVA ZA PODRŠKU

Ovde su navedeni svi tipovi imovine koju treba identifikovati i opisati. Sva ova imovina ima ranjivosti koje pretnje mogu iskoristiti sa ciljem da se ugrozi primarna imovina područja primene zaštite (poslovni procesi i informacije).

D-2.1 Hardver

Hardver je tip imovine koja sadrži sve fizičke elemente nekog procesa.

D-2.1.1 Oprema za obradu podataka (aktivna)

Računarska oprema za automatsku obradu podataka, uključujući delove potrebne za nezavisan rad.

D-2.1.2 Prenosiva oprema

Prenosiva računarska oprema (laptop, PDA).

D-2.1.3 Fiksna oprema

Računarska oprema koja se koristi u prostorijama organizacije.

D-2.1.4 Periferna oprema

Računarska oprema povezana sa računarom putem komunikacionog porta (serijski ili paralelna veza i sl.) za unos, transport ili prenos podataka (npr. štampač, prenosivi hard disk).

D-2.1.5 Pasivni medijumi

Medijumi za skladištenje podataka.

D-2.1.6 Elektronski medijumi

Medijumi za skladištenje podataka koji mogu da se konektuju na računar ili računarsku mrežu. I pored kompaktne veličine, ovi medijumi mogu da sadrže ogromne količine podataka. Oni mogu da se koriste sa standardnom računarskom opremom. PRIMERI: floppy disk, CD/DVD, Backup kertridž, prenosivi hard disk, memorijski ključ, magnetna traka, itd.

D-2.2 Softver

Softveri su svi programi koji učestvuju u obradi podataka.

D-2.2.1 Operativni sistem

Svi programi koji predstavljaju operativnu osnovu na kojoj se izvršavaju ostali programi (servisi ili aplikacije). Operativni sistem sadrži kernel i osnovne funkcije servisa. U zavisnosti od arhitekture, operativni sistem može biti monolitni ili da je sastavljen od micro-kernel i skupa sistemskih servisa. Glavni elementi operativnog sistema su:

- servisi za upravljanje svim delovima računara (CPU, memorija, disk, mrežni interfejs),
- task ili servisi za upravljanje procesima i
- servisi za upravljanje korisničkim pravima.

D-2.2.2 Softveri za održavanje ili administraciju

Softver koji dopunjuje servise operativnog sistema i nije direktno u službi korisnika ili aplikacija (iako obično od suštinskog značaja ili čak neophodan za funkcionisanje informacionog sistema).

D-2.2.3 Standardni softver ili softverski paket

Standardni softver ili softverski paket je kompletan komercijalni proizvod (nije proizveden za jednokratnu ili specifičnu upotrebu) sa medijumom, verzijom i podrškom. On nudi servise korisnicima i aplikacijama, ali nije personalizovan ili specifičan za

određenu poslovnu aplikaciju. PRIMERI: softver za upravljanje bazama podataka, softver za razmenu elektronskih poruka, softver za radne timove, softver za direktorijume, softver za web servere, itd.

D-2.2.4 Poslovna aplikacija

Standardna poslovna aplikacija

Komercijalni softver dizajniran da omogući korisniku direktan pristup servisima ili funkcijama koje zahtevaju od svog informacionog sistema u profesionalnom smislu. Imaju veoma široku, teoretski neograničenu, primenu. PRIMERI: softver za računovodstvo, softver za kontrolu mašine alatke, softver za korisničku podršku, softver za upravljanje kompetencijama osoblja, administrativni softver, itd.

Specifična poslovna aplikacija

Namenski razvijen softver koji korisnicima daje direktan pristup servisima i funkcijama koje zahtevaju od informacionog sistema. Imaju veoma široku, teoretski neograničenu, primenu. PRIMERI: fakturisanje klijenata telekomunikacionih usluga, aplikacija za praćenje lansiranja rakete.

D-2.3 Mreža

Mreža je tip imovine koji uključuje sve telekomunikacione uređaje koji se koriste za međusobno povezivanje fizički udaljenih računara ili elemenata informacionog sistema.

D-2.3.1 Medijumi i podrška

Komunikacioni i telekomunikacioni medijumi ili oprema za koju se uglavnom posmatraju fizičke i tehničke karakteristike opreme (point-to-point, broadcast) i komunikacioni protokoli (link ili mreža – nivoi 3 i 3 OSI 7–layer modela). PRIMERI: public Switching Telephone Network (PSTN), Ethernet, GigabitEthernet, Asymmetric Digital Subscriber Line (ADSL), wireless protocol specifications (npr. WiFi 802.11), Bluetooth, FireWire.

D-2.3.2 Pasivni ili aktivni relej

Ovaj podtip podrazumeva sve tipove uređaja koji nisu logički komunikacioni završeci (IS vizija), nego su posredni relejni uređaji. Releji se karakterišu komunikacionim protokolima podržavane mreže. Pored osnovnog releja, često uključuju rutiranje i/ili funkcije filtriranje i servise, koriste komunikacione svičeve i rutere sa filterima. Takođe, često mogu da se administriraju sa udaljenosti i obično su u stanju da generišu logove. PRIMERI: bridge, router, hub, switch, automatic exchange.

D-2.3.3 Komunikacioni interfejs

Komunikacioni interfejsi procesorskih jedinica povezani su sa procesorskim jedinicama, ali se karakterišu medijumima i podržavanim protokolima, bilo kakvim instaliranim filtriranjem, funkcijama logovanja ili generisanja upozorenja i svojim kapacitetima, mogućnostima i zahtevima za udaljenom administracijom. PRIMERI: general Packet Radio Services (GPRS), Ethernet adapter.

D-2.4 Personal

Personal je tip imovine koja podrazumeva sve grupe ljudi uključenih u informacioni sistem UC.

D-2.4.1 Donosilac odluke

Donosioci odluka su vlasnici primarne imovine (informacija i funkcija) i rukovodioci određenih projekata organizacije PRIMERI: glavno rukovodstvo, vođa tima.

D-2.4.2 Korisnik

Korisnici su osoblje koje rukuje osetljivim elementima u kontekstu svojih aktivnosti i imaju posebne odgovornosti s tim u vezi. Za obavljanje svojih svakodnevni zadataka korisnici mogu da imaju posebna prava pristupa u informacionom sistemu. PRIMERI: menadžment ljudskim resursima, finansijski menadžment, rukovodilac rizikom.

D-2.4.3 Osoblje za operativni rad i održavanje

Osoblje zaduženo za operativni rad i održavanje informacionog sistema. Za obavljanje svojih svakodnevni poslova potrebna su im specijalna prava pristupa informacionom sistemu. PRIMERI: administratori sistema, administratori podataka, back-up, Help Desk, operater za razvoj aplikacija, službenici za bezbednost.

D-2.4.4 Programer

Programeri su zaduženi za razvoj poslovnih aplikacija organizacije. Imaju pristup delu informacionog sistema sa visokim pravima, ali ne rade ništa sa produkcionim podacima, ili ih kontrolisano koriste u svrhe testiranja.

D-2.5 Lokacija

Sva mesta koja su obuhvaćena područjem primene zaštite ili delom područja i gde su fizički smeštena radna sredstva.

D-2.5.1 Spoljašnje okruženje

Spoljašnje okruženje se odnosi na sva mesta gde organizacija ne može da primeni zaštitu. PRIMERI: domovi osoblja, prostorije druge organizacije, okruženje van sedišta (gradska oblast, opasne zone).

D-2.5.2 Prostor

Mesta koja su od direktnog kontakta sa spoljnim svetom razdvojena perimetrima organizacije, koji mogu biti zaštićeni fizičkim barijerama ili sredstvima za nadzor oko zgrada. PRIMERI: ustanova, zgrade.

D-2.5.3 Zona

Zone su unutar prostora organizacije formirane fizičkim granicama zaštite. Nastaju postavljanjem fizičkih barijera oko infrastrukture za obradu informacija. PRIMERI: kancelarije, rezervisana zona pristupa, zaštićena zona.

D-2.5.4 Glavni servisi

Svi servisi neophodni za funkcionisanje informacionih resursa.

D-2.5.5 Komunikacija

Telekomunikacioni servisi i oprema koju obezbeđuje operater. PRIMERI: telefonska linija, PABX (Private Automatic Branch Exchange), interne telefonske mreže.

D-2.5.6 Pomoćna sredstva

Servisi i sredstva (napajanje i kablovi) potrebno za napajanje opreme informacionih tehnologija i periferija. PRIMERI: niskonaponsko napajanje, inverter, električno kolo,

Vodovod i kanalizacija.

Odlaganje otpada.

Servisi i sredstva (oprema, kontrola) za hlađenje i pročišćavanje vazduha. PRIMERI: rashladne cevi sa vodom, klima uređaji.

D-2.6 Organizacija

Ovaj tip opisuje organizacioni okvir koji se sastoji od svih struktura personala koji imaju delegiran zadatak i procedure za kontrolu ovih strukture.

D-2.6.1 Autoritet

To su organizacije preko kojih posmatrana organizacija ostvaruje svoj autoritet. Mogu biti pravno povezani ili eksterni. Ovo nameće ograničenja posmatranoj organizaciji u smislu regulativa, odlučivanja i preduzimanja akcija. PRIMERI: administrativno telo, sedište organizacije.

D-2.6.2 Organizaciona struktura

Sastoji se od različitih oblasti organizacije, uključujući i njihove međusobne funkcionalne aktivnosti, pod kontrolom svog rukovodstva. PRIMERI: upravljanje ljudskim resursima, IT menadžment, nabavka, prodaja, fizičko obezbeđenje, audit menadžment.

D-2.6.3 Projektna ili sistemska organizacija

Odnosi se na specifičan projekat ili servis organizacije. PRIMERI: projekat razvoja nove aplikacije, outsourcing kompanija, konsultantska kompanija.

D-2.6.4 Podugovarači / Dobavljači / Proizvođači

Organizacije koje pod ugovorom obezbeđuju servise ili resurse i vezani su ugovorom. PRIMERI: kompanija za održavanje objekata, outsourcing kompanija, konsultantska kompanija.

PRILOG E. PRIMENA APLIKACIJE “APPRAISAL ASSISTANT” ZA UNAPREĐENJE PROGRAMA MERENJA ZAŠTITE

Appraisal Assistant je softverski alat koji služi za podršku u analizi i oceni zrelosti procesa organizacije i poboljšavanju njihovih kapaciteta. Metodološki pristup se oslanja na zahteve međunarodnog standarda za informacione tehnologije ISO/IEC 15504, poznatijeg kao *SPICE: Process assessment, and the Assessment Requirements for CMMI®*¹⁴.

Za razliku od ostalih dostupnih alata, rezultati koje generiše *Appraisal Assistant*, eksplicitno se zasnivaju na informacijama (dokazima) prikupljenim u toku evaluacije (na bazi strogo utvrđenih kriterijuma SCAMPI metoda evaluacije procesa¹⁵), odnosno, zbog širokog spektra karakterizacije dokaza isključuje bilo kakvu subjektivnu komponentu, koja je uobičajena kod alata koji se koriste za kvalitativnu procenu.

Appraisal Assistant podržava:

- Različite modele procesa – ISO/IEC 15504-5, ISO/IEC 15504-6 (FDIS), Automotive SPICE, CMMI®-DEV v.1.2, +SAFE i CMMI SE/SW/PPD/SS V 1.1;
- Korisnički definisane modele – *moгуćnost koja je iskorišćena u ovom primeru*;
- Različite metode izvođenja evaluacije, uključujući SCAMPISM A (v.1.2) i B Class i generičke ISO/IEC 15504 modele evaluacije usaglašenosti.
- Korisnički definisane metode evaluacije;
- Konverziju rezultata iz jednog okvira u drugi. Na primer, rezultati CMMI® evaluacije procesa predstavljeni prema ISO 15504 profilu procesa i definisanje pokrivenosti ISO 9001 zahteva putem CMMI® ili ISO 15504 evaluacije procesa – *moгуćnost koju koriste softverske kompanije, kako bi mapirale svoje procese sa zahtevima standarda ISO 9001*.
- Uspostavljanje mini-timova, što omogućava timsko prikupljanje, podelu i konsolidaciju prikupljenih dokaza.
- Automatsko generisanje raznih izveštaja, uključujući izjavu o neotkrivanju informacija sa evaluacije, PIID, zapise i nalaze evaluacije, pregled prednosti i nedostataka, profili zrelosti i radni zadaci.
- Automatske izveštaje pokrivenosti modela prikupljenim dokazima prema zahtevima metoda SCAMPISM A v.1.2.

Što se tiče prava intelektualne svojine, ©*Appraisal Assistant* je vlasništvo Griffith univerziteta, SM SCAMPI je zaštitni znak Carnegie Mellon univerziteta, ®CMMI je patent registrovan u U.S. zaštitni znak Carnegie Mellon univerziteta.

Kao što je pomenuto u prethodnom poglavlju, *Appraisal Assistant* dozvoljava da korisnik definiše novi model procesa u odnosu na koji će meriti zrelost i kapacitete za poboljšanje procesa svoje organizacije. U ovom slučaju, aplikacija je obogaćena još jednim modelom procesa, SSE-CMM¹⁶ modelom sazrevanja procesa zaštite informacija. Ovaj model je izrađen na osnovu međunarodnog standarda ISO/IEC 21827¹⁷, koji opisuje osnovne karakteristike sistemskih procesa bezbednosnog inženjeringa i može da se koristi kao:

- Alat za evaluaciju i definisanje poboljšanja inženjerskih praksi zaštite;

¹⁴ [Software Process Improvement and Capability Determination](#)

¹⁵ [Standard CMMI Appraisal Method for Process Improvement](#)

¹⁶ [Systems Security Engineering Capability Maturity Model \(SSE-CMM\)](#)

¹⁷ [ISO/IEC 21827 Information technology – Security techniques – Systems security engineering – Capability maturity model \(SSE-CMM\)®](#)

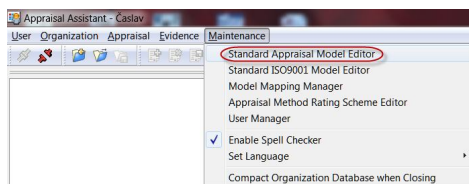
- Standardni mehanizam za klijenta koji želi da evaluiira bezbednosne kapacitete davaoca usluga;
- Osnova za evaluaciju bezbednosnog inženjeringa organizacije (npr. sertifikatori sistema i evaluatori proizvoda), kako bi se uspostavilo poverenje u organizaciju zasnovano na nivou kapaciteta (kao deo systemske ili projektne bezbednosne garancije);
- Mehanizam za upravljanje aktivnostima bezbednosnog inženjeringa koji obuhvataju sve proizvode zaštite ili životni ciklus sistema zaštite, uključujući definisanje koncepta, analizu zahteva, dizajn, razvoj, integraciju, instalaciju, operativni rad, održavanje i povlačenje iz upotrebe;
- Mehanizam za primenu bezbednosti u programiranju, razvoju sistema, integrisanju i organizaciji proizvodnje servisa zaštite i bezbednosnog inženjeringa;

SSE-CMM može da se primeni na sve tipove i veličine bezbednosno inženjerskih organizacija (komercijalne, vladine i akademske), a u ovom primeru biće demonstriran način njegove primene u bilo kojoj organizaciji koja ima sistem upravljanja zaštitom informacija.

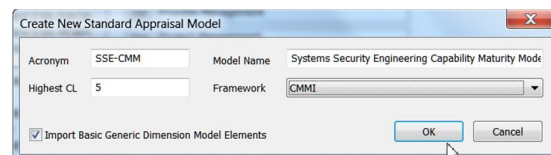
U ovom primeru naziv projekta evaluacije je “Projekat poboljšanja procesa procene uticaja bezbednosnog rizika”, koji ima za cilj da organizacija:

1. Izmeri nivo organizacione zrelosti za merenje uticaja bezbednosnih rizika;
2. Organizacionim merama poboljša kapacitete procesa procene uticaja; i
3. Izvrši procenu bezbednosnog uticaja i te rezultate koristi za unapređenje programa merenja sistema za upravljanje zaštitom informacija.

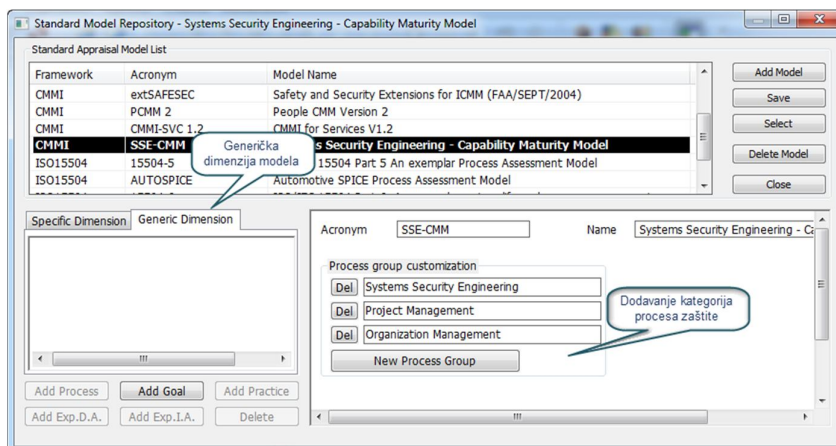
Korak 1 Model editor



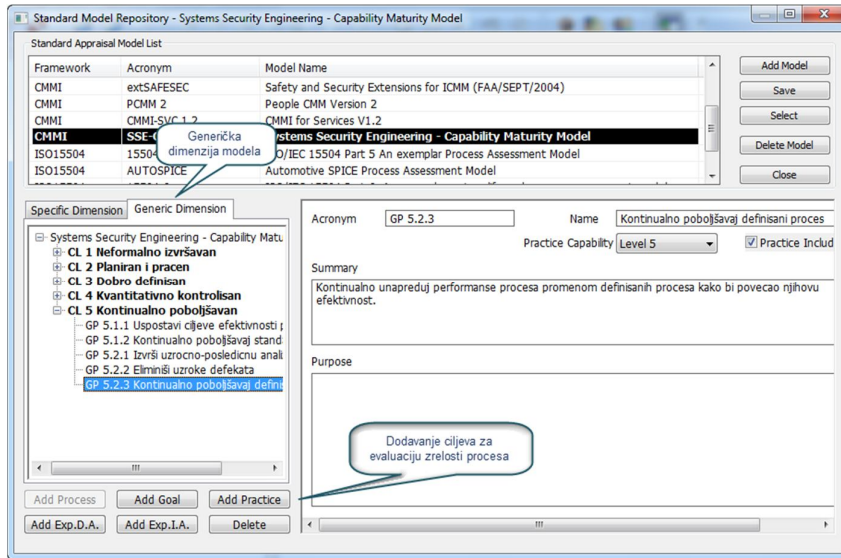
Korak 2 Dodavanje novog modela – Naziv modela, skraćenica, najviši nivo zrelosti procesa



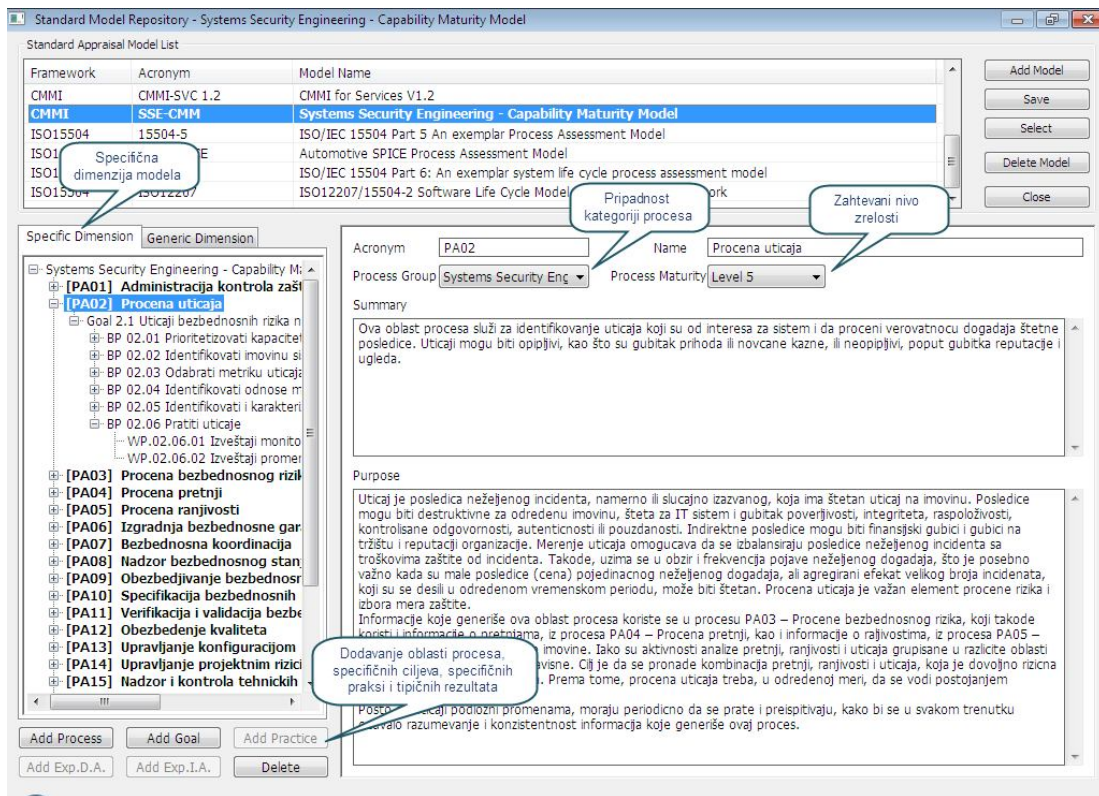
Korak 3 Generička dimenzija modela – Definisanje kategorija procesa zaštite informacija



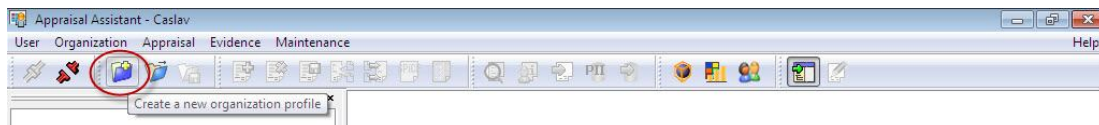
Korak 4 Generička dimenzija modela – Definisanje uslova ispunjenja nivoa zrelosti procesa



Korak 5 Specifična dimenzija modela – Definisanje procesa zaštite, pridruživanje grupi procesa i utvrđivanje zahtevanog nivoa zrelosti procesa



Korak 6 Pokretanje procesa unosa podataka o organizaciji u kojoj se primenjuje projekat poboljšanja procesa procene bezbednosnog uticaja



Korak 7 Osnovni podaci o evaluiranoj organizaciji

New Organization Profile

Data Location: D:\Master Browse

Organization Name: Organizacija

Address: Neznanog junaka bb

Contact Person: Direktor

Email: direktor@org.rs

Phone: 555-2856 Fax: 555-28561

OK Cancel

Korak 8 Definisanje profila organizacije – Detalji o tipu i delatnosti privrednog subjekta; izbor modela procesa; izbor rigoroznosti metoda karakterizacije dokaza provere; izbor načina prezentovanja rezultata evaluacije (kontinualna – predefinisani nivo zrelosti procesa (profil nivoa zrelosti), fazna – svi procesi na istom nivou zrelosti)

Appraisal Assistant - Caslav - Organizacija

User Organization Appraisal Evidence Maintenance Help

Create a new appraisal for the current organization unit

Organization

Organization Name: Organizacija

Address: Neznanog junaka bb

Contact: Direktor

E-mail: direktor@org.rs

Phone: 555-2856

Fax: 555-28561

Organization Context

New Appraisal Project

Name: Projekat poboljšanja procesa procene bezbednosnog uticaja

Framework: CMMI Staged

Target ML: Level 5

Method: SCAMPI A v1.2

Table:

Acronym	Name
☐ CMMI-Dev 1.2	CMMI for Development V1.2
☐ CMMI-ACQ 1.2	CMMI for Acquisition V 1.2
☐ PCMM 2	People CMM Version 2
☐ CMMI-SVC 1.2	CMMI for Services V1.2
☒ SCMM	Systems Security Engineering - Capability ...

OK Cancel

Appraisal Project List

Project	Date

Create a new appraisal for the current organizatio

Callouts:

- Naziv projekta
- Izbor metoda evaluacije
- Tip i delatnost privrednog subjekta
- Izbor načina prezentovanja rezultata evaluacije
- Izbor modela

Korak 9 Definisanje projekta evaluacije i evaluiranih projekata organizacije

Appraisal Assistant - Časlav - Organizacija - Projekat poboljšanja procesa procene uticaja bezbednosnog rizika - SCAMPI A v1.2

User Organization Appraisal Evidence Maintenance Help

Organization Appraisal Model

Projekat poboljšanja procesa procene uticaja

Opis projekta evaluacije

Evaluirani projekti organizacije (instance u kojima se pojavljuju dokazi evaluacije)

Appraisal Customization Practice Characterization Goal Process Area Organization Unit Appraisal Result

Appraisal Project Name: Projekat poboljšanja procesa procen Appraisal Sponsor: Direktor Appraisal Date: 17. 3.2010

Project Purpose/Summary/Constraints

Projekat poboljšanja procesa procene uticaja bezbednosnog rizika da organizacija:

1. Izmeni nivo organizacione zrelosti za merenje uticaja bezbednosnih rizika;
2. Organizacionim merima poboljša kapacitete procesa procene uticaja; i
3. Izvrši procenu bezbednosnog uticaja i te rezultate koristi za unapređenje programa merenja sistema za upravljanje zaštitom informacija.

Appraisal Organizational Scope

Process Instantiations (Projects)

Name: Program merenja zaštite informacija

Context:

Map Practice

Delete

Add Instantiation

Dodavanje/brisanje procesa modela i specifičnih praksi procesa

Appraisal Model Scope

Processes and Target Capability Levels

Process Area Target Capability

Delete Add Customize

Appraisal Team

Login Name	Role	Organization
Časlav Maksić	Team Leader	
Pera perić	Team Member	XYZ
Marko Marković	Team Member	

Delete Add

Evaluatori

Saving ISO9001:2000 profile ...

Korak 10 Izbor procesa za upravljanje bezbednosnim rizikom, koji će biti evaluirani i poboljšani

Add CMMI Process Areas to the Project

CMMI Process Areas

- PA01 Administracija kontrole zaštite
- PA02 Procena uticaja
- PA03 Procena bezbednosnog rizika
- PA04 Procena pretnji
- PA05 Procena ranjivosti
- PA06 Izgradnja bezbednosne garancije
- PA07 Bezbednosna koordinacija
- PA08 Nadzor bezbednosnog stanja
- PA09 Obezbeđivanje bezbednosnog ulaza
- PA10 Specifikacija bezbednosnih potreba
- PA11 Verifikacija i validacija bezbednosti
- PA12 Obezbeđenje kvaliteta
- PA13 Upravljanje konfiguracijom
- PA14 Upravljanje projektnim rizicima
- PA15 Nadzor i kontrola tehničkih aktivnosti
- PA16 Plan tehničkih aktivnosti
- PA17 Definisanje inženjerskih procesa zaštite organizacije
- PA18 Poboljšavanje inženjerskih procesa zaštite organizacije
- PA19 Upravljanje evolucijom proizvodne linije
- PA20 Upravljanje okruženjem za podršku sistemskog inženjerstva
- PA21 Obezbeđenje tekucih veština i znanja
- PA22 Koordinacija sa dobavljačima

Default C.L. 5

Select All

Clear All

OK

Cancel

Dodavanje procesa iz modela, koji će biti evaluirani i poboljšani

Add

Korak 11 Utvrđivanje profila zrelosti evaluiranih procesa organizacije

Appraisal Assistant - Časlav - Organizacija - Projekat poboljšanja procesa procene uticaja bezbednog rizika - SCAMPI A v1.2

User Organization Appraisal Evidence Maintenance

Appraisal Customization Practice Characterization Goal Process Area Organization Unit Appraisal Result

Appraisal Project Name: [Projekat poboljšanja procesa procene uticaja] Appraisal Sponsor: Direktor 17. 3. 2010

Project Purpose/Summary/Constraints

Projekat poboljšanja procesa procene uticaja bezbednog rizika ima za cilj da organizacija:

1. Izmeni nivo organizacione zrelosti za merenje uticaja bezbednosnih rizika;
2. Organizacionim merama poboljša kapacitete procesa procene uticaja;
3. Izvrši procenu bezbednog uticaja i te rezultate koristi za unapređenje programa merenja sistema za upravljanje zaštitom informacija.

Appraisal Organizational Scope

Process Instantiations (Projects)

Name: Program merenja zaštite informacija

Context:

Map Practice

Delete

Add Instantiation

Appraisal Model Scope

Processes and Target Capability Levels

Process Area	Target Capability
PA02 - Procena uticaja	Level 5
PA03 - Procena bezbednosnog rizika	Level 3
PA04 - Procena pretnji	Level 3
PA05 - Procena ranjivosti	Level 5
PA06 - Izgradnja bezbednosne garancije	Level 3
PA08 - Nadzor bezbednosnog stanja	Level 5
PA09 - Obezbeđivanje bezbednosnog ul...	Level 4
PA10 - Specifikacija bezbednosnih potreba	Level 3

Delete Add Customize

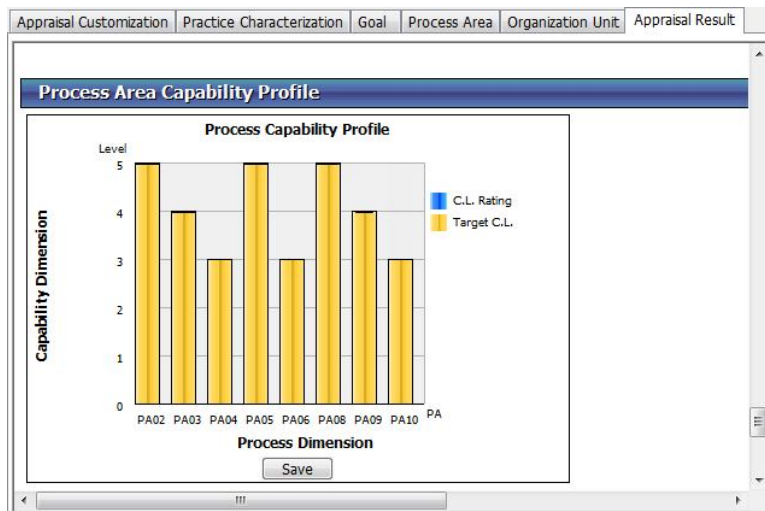
Appraisal Team

Login Name	Role	Organization

For Help, press F1

NUM

Korak 12 Zadati nivo zrelosti procesa



Korak 13 Otvaranje registra dokaza evaluacije

Organizacija - Projekat poboljšanja procesa procene u

Evidence Maintenance

Evidence Registry

Notes of Cross-Instantiation Evidences

Export List of Exemplar Work products

Create Initial Evidence Collection Spreadsheet

Import Initial Evidences

Export Evidence Database

Import Evidence Database

Bookmark Recently Modified PIIs

[illegible]

Evidence Registry

Evidence List

Evidence	Instantiation
Metric	Program merenj...
Plan merenja	Program merenj...
Izveštaji promena...	Multi-Inst
Izveštaji monitori...	Multi-Inst
Lista zloštenosti u...	Program merenj...
Pravila kombinova...	Multi-Inst
Ista međumetrič...	Multi-Inst
Metrika uticaja	Program merenj...
Imovina sistema	Program merenj...
Produkciona mov...	Multi-Inst
Profil kapaciteta s...	Multi-Inst
Prioriteti sistema	Multi-Inst

Dokazi implementacije preakisi i kapaciteta procesa

Evidence Detail Information

Associate the Metric of Program merenja zaštite informacija to model practices

Evidence to CMMI Practice Association

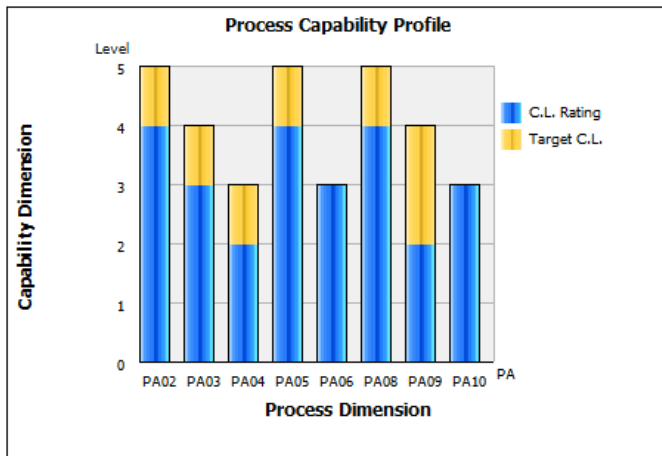
Appraisal Model	Indicator Type	Adequacy	Characteristic	By
PA02 Procena uticaja				
Goal 2.1 Uticaji bezbednosnih rizika n...				
PA02 BP 02.01 Prioritetizovati u...				
Inst: Program merenja zaštite i...		Strong Evidence	Fully Implemented	Esaslav Mal
Prioriteti sistema	Direct Artifact		Strength	Esaslav Mak
Profil kapaciteta sistema	Direct Artifact		Strength	Esaslav Mak
PA02 BP 02.02 Identifikovati i...				
PA02 BP 02.03 Odabrati metrič...				
PA02 BP 02.04 Identifikovati o...				
PA02 BP 02.05 Identifikovati i ...				
PA02 BP 02.06 Prati uticaje				
CL 1 Neformalno izvrsavan				
CL 2 Planiran i pracen				
CL 3 Dobro definisan				
CL 4 Kvantitativno kontrolisan				
CL 5 Kontinualno poboljšavan				
PA03 Procena bezbednosnog rizika				
PA04 Procena pretnji				

Legend:

- Not Yet Reviewed
- Strong Evidence
- Not Allocated
- Direct Artifact
- Indirect Artifact
- Insufficient Evidence
- Conflicting Evidence
- Anomalous Evidence
- Strength/Weakness
- Not Characterized
- Not Yet Implemented
- Partially Implemented
- Largely Implemented
- Fully Implemented

Evidence Detail Information	Evidence to CMMI Practice Association	Model Practices Evidence Coverage
Appraisal Model evidence coverage		
The numbers of indicator are displayed as: num. DirectArtifact - num. IndirectArtifact - num. Affirmation (Total num. PII)		
Appraisal Model	Instance 1	
PA02 Procena uticaja		
Goal 2.1 Uticaji bezbednosnih rizika na sistem su identifikovani i karakterizovani.		
BP 02.01 Prioritetizovati kapacitete	2	0 - 0 (2)
BP 02.02 Identifikovati imovinu sistema	0	0 - 0 (0)
BP 02.03 Odabrati metriku uticaja	0	0 - 0 (0)
BP 02.04 Identifikovati odnose među metrikama	0	0 - 0 (0)
BP 02.05 Identifikovati i karakterizovati uticaje	0	0 - 0 (0)
BP 02.06 Pratiti uticaje	0	0 - 0 (0)
CL 1 Neformalno izvršavan		
GP 1.1.1 Izvrši proces	0	0 - 0 (0)
CL 2 Planiran i pracen		
GP 2.1.1 Alociraj resurse	0	0 - 0 (0)
GP 2.1.2 Delegiraj odgovornosti	0	0 - 0 (0)
GP 2.1.3 Dokumentuj proces	0	0 - 0 (0)
GP 2.1.4 Obezbedi alate	0	0 - 0 (0)
GP 2.1.5 Obezbedi obuku	0	0 - 0 (0)
GP 2.1.6 Planiraj proces	0	0 - 0 (0)
GP 2.2.1 Koristi planove, standarde i procedure	0	0 - 0 (0)
GP 2.2.2 Upravljaj konfiguracijom	0	0 - 0 (0)
GP 2.3.1 Verifikuj usklađenost procesa	0	0 - 0 (0)
GP 2.3.2 Kontroliši proizvode rada	0	0 - 0 (0)
GP 2.4.1 Prati sa merenjem	0	0 - 0 (0)
GP 2.4.2 Preduzmi korektivne akcije	0	0 - 0 (0)
CL 3 Dobro definisan		
GP 3.1.1 Standardizuj proces	0	0 - 0 (0)

Korak 17 Rezultat evaluacije procesa – Evaluirani profil zrelosti (plavo). Kontinualna reprezentacija zrelosti pojedinačnih procesa



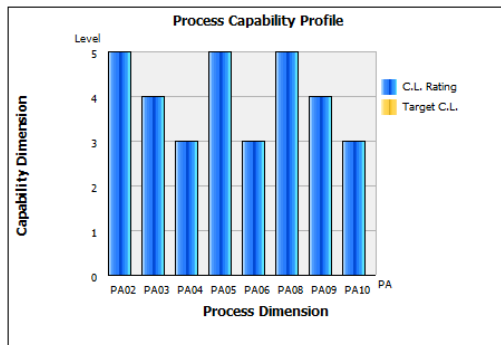
Korak 18 Srednja ocena implementacije praksi, prema kategoriji procesa (u ovom primeru samo jedna kategorija – inženjerski procesi zaštite)



Korak 19 Fazna reprezentacija evaluirane zrelosti grupe procesa

Appraisal Customization	Practice Characterization	Goal	Process Area	Organization Unit	Appraisal Result			
Projekat poboljšanja procesa procene uticaja bezbednosnog rizika								
Projekat poboljšanja procesa procene uticaja bezbednosnog rizika ima za cilj da organizacija: 1. Izmeri nivo organizacione zrelosti za merenje uticaja bezbednosnih rizika; 2. Organizacionim merama poboljša kapacitete procesa procene uticaja; i 3. Izvrši procenu bezbednosnog uticaja i te rezultate koristi za unapređenje programa merenja sistema za upravljanje zaštitom informacija.								
Organization Unit Maturity Rating :				ML4 - Quant. Managed				
CMMI Equivalent Staging Table								
Model	Process Area	Acronym	ML	CL1	CL2	CL3	CL4	CL5
SSE-CMM	Procena pretnji	PA04	3					
SSE-CMM	Izgradnja bezbednosne garancije	PA06	3					
SSE-CMM	Specifikacija bezbednosnih potreba	PA10	3					
SSE-CMM	Procena bezbednosnog rizika	PA03	4					
SSE-CMM	Obezbedjivanje bezbednosnog ulaza	PA09	4					
SSE-CMM	Procena uticaja	PA02	5					
SSE-CMM	Procena ranjivosti	PA05	5					
SSE-CMM	Nadzor bezbednosnog stanja	PA08	5					

Korak 20 Profil zrelosti nakon poboljšavanja kapaciteta procesa



Korak 21 Fazna reprezentacija unapredene zrelosti grupe procesa

Model	Process Area	Acronym	ML	CL1	CL2	CL3	CL4	CL5
SSE-CMM	Procena pretnji	PA04	3					
SSE-CMM	Izgradnja bezbednosne garancije	PA06	3					
SSE-CMM	Specifikacija bezbednosnih potreba	PA10	3					
SSE-CMM	Procena bezbednosnog rizika	PA03	4					
SSE-CMM	Obezbedjivanje bezbednosnog ulaza	PA09	4					
SSE-CMM	Procena uticaja	PA02	5					
SSE-CMM	Procena ranjivosti	PA05	5					
SSE-CMM	Nadzor bezbednosnog stanja	PA08	5					

5 LITERATURA

- [1] Andrew Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, Pearson Education, Inc., March 2007.
<http://www.securitymetrics.org/content/Wiki.jsp>
- [2] Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems and Organizations*, Special Publication 800-53 Revision 3, August 2009, <http://csrc.nist.gov/publications/PubsSPs.html>
- [3] Debra S. Herrmann, *Complete guide to security and privacy metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI*, Auerbach Publications Taylor & Francis Group, LLC, 2007.
- [4] Dennis Opacki, CISSP, dopacki@covestec.com, *Security Metrics: Building Business Unit Scorecards*, December 2005.
- [5] Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Laurie Graffo, *Performance Measurement Guide for Information Security*, NIST Special Publication SP800-55-rev1, July 2008.
<http://csrc.nist.gov/publications/PubsSPs.html>
- [6] Gary Stoneburner, Alice Goguen, and Alexis Feringa, *Risk Management Guide for Information Technology Systems*, NIST Special Publication SP800-30, Jul 2002.
- [7] Gerald L. Kovacich and Edvard P. Halibocek, *Security metrics management: how to measure the costs and benefits of security*, 2006.
- [8] Information Security Forum (ISF), *Information Security Metrics – Report*, May 2006, <http://www.securityforum.org/>
- [9] ISO/IEC 27004:2009 *Information technology — Security techniques — Information security management — Measurement*. <http://www.iso.org/iso/>
- [10] ISO27k forum, <http://www.iso27001security.com/html/forum.html>.
- [11] Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, and Laurie Graffo, *Security Metrics Guide for Information Technology Systems*, NIST Special Publication 800-55, July 2003.
- [12] Milan M., Gojko G., *Osnovi bezbednosti i zaštite informacionih sistema*, Univerzitet Singidunum, 2006.
- [13] Pauline Bowen, Richard Kissel, Matthew Scholl, Will Robinson, Jessica Stansfield, Lisa Voldish, *Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process (CPIC)*, NIST Special Publication 800-65 (draft), 14. Avgust, 2009.
- [14] Shirley C. Payne, *A Guide to Security Metrics*, SANS Institute, InfoSec Reading Room, June 19, 2006. http://www.sans.org/reading_room/whitepapers/auditing/