

METRIČKI SISTEMI U OBLASTI ZAŠTITE INFORMACIJA

Mr Gojko Grubor, dipl. inž. el., FPI, Univerzitet SINGIDUNUM

Kratak sadržaj: *Sistem kvaliteta zaštite informacija čine brojne metrike performansi sistema zaštite i usklađenosti procesa zaštite sa standardima i politikama zaštite. Glavni cilj metrike sistema zaštite je uspostavljanje kvaliteta kontrolisanog, ponovljivog i stabilnog procesa upravljanja zaštitom, što je od presudnog značaja za izvođenje dokaznog postupka u slučaju kompjuterskog incidenta i kompjuterskog kriminala. U procesnom pristupu zaštiti informacija, SSE CMM model za merenje zrelosti procesa zaštite i upravljanje programom zaštite informacija, daje dobre rezultate.*

Abstract: *Quality system of information security is made of the metrics of numerous security system performance and compliances of the security processes with the security standards and policies. To establish a qualifiable, controlable, repetitive and stable processes of the security system management is the main objective of the security metric system. In particular, it is of the critical importance for forensic acquisition and analysis of digital evidence in the computer incidents and crimes cases. In a process approach to information security, the SSE CMM model and method seems to offer the best results.*

Ključne reči: *merenje, metrika, metrički sistem, SSE CMM model, zrelost procesa.*

1. METODOLOGIJA SISTEMA MERENJA ZAŠTITE INFORMACIJA

UVOD

U sistemu zaštite informacija ni jedna aktivnost ne može biti dobro upravljana ako se ne može izmeriti. Ciljevi zaštite *raspoloživosti, integriteta i poverljivosti* informacija, primarno usmereni na zaštitu informacija u informaciono-komunikacionom (IKT) sistemu, mogu se odrediti na bazi: *bezbednosnih zahteva* (n.p.r., **ISO/IEC 15408, CC**), *kontrola najbolje prakse zaštite* (n.p.r., **ISF V.4**), *sistema osnovnih kontrola zaštite* (n.p.r., **ISO/IEC 17799**), *upravljanja sistemom zaštite* na bazi iskustva (poboljšavanjem procesa zaštite) i primene metrike *modela progresivnog sazrevanja procesa zaštite* (n.p.r., **SSE-CMM**), [4].

Razvoj programa metričkog sistema zaštite uključuje izbor metodologije: definisanje objekata zaštite za merenje, izbor tipa, razvoj procesa i implementaciju metričkog sistema. Dobra metodologija metrike zaštite zahteva poznavanje i primenu generičkog procesa metričkog sistema. Između više metodologija za testiranje i garanciju kvaliteta proizvoda i sistema zaštite, pažnju zaslužuje model i metod za progresivni razvoj sazrevanja procesa zaštite-**SSE-CMM** (*System Security Engeneering Capability Maturity Model*). U Standardu **ISO/IEC 15443** navedene su sve metode i sredstva za kontrolu kvaliteta i to bazirane na: **procesnom pristupu** (**SSE-CMM**, **ISO 9000-3**, **ISO 9001**, **ISO/IEC 15504** i.t.d.), **pristupima proizvod/sistem/servis** zaštite (**CC/CEM**, **ITSEC/ITSEM**, **TCSEC/TPEP**, **ISO/IEC 9646**, **ISO/IEC 14598** i dr.) i na **pristupu okruženju** (**TCMM**, **ISO 13407** i dr.).

1.1. Definicije pojmova

Merenje se definiše kao jednokratni uvid u specifične merne parametre komponente/sistema zaštite. U praksi zaštite razvijeno je više metoda za merenja nivoa zaštićenosti informacija: analiza rizika; kontrola (*auditing*); sertifikacija; merenje upada u sistem (**IDS/IPS**); nadzor performansi sistema zaštite (mrežni skeneri); testiranje sistema na proboj (simulacija malicioznih napada) i.t.d. U svim ovim metodima koriste se brojne **metrike** i **metrički sistemi**.

Metrika je višekratno merenje u dužem vremenskom periodu ili sredstvo za interpretaciju agregiranih podataka merenja (mernih podataka) na višem nivou (organizacije). Zahtevani merni podaci moraju biti dostupni, a razmatrani procesi merljivi, konzistentni, stabilni i ponovljivi. Metrika mora obezbediti kvantitativne **merne jedinice** koji se mogu upoređivati, od jednog do drugog merenja i primenjivati za analizu i praćenje promena korišćenjem istih referentnih mernih vrednosti, najčešće: **procentni račun**, **srednja vrednost** i **apsolutni brojevi**. Metrika monitoriše stepen postizanja taktičkih (*goals*) i strateških (*objecives*) ciljeva zaštite: kvantifikovanjem nivoa implementacije, efektivnosti i efikasnosti kontrola zaštite; analizom adekvatnosti procesa i kontrola zaštite i identifikovanjem mogućih akcija za njihovo poboljšavanje, [10].

Primer: „Svi zaposleni moraju završiti adekvatni kurs i usvojiti program za podizanje svesti o potrebi zaštite“ (**Strateški cilj**), a odgovarajući **taktički ciljevi**: „Svi novi zaposleni moraju završiti program obuke za novo zaposlene“, „Obuka zaposlenih uključuje osnove Pravila i ponašanja u IKT sistemu“ i „Obuka zaposlenih uključuje osnove politika i procedura zaštite na nivou organizacije“.

Metrički sistem je skup kriterijuma, parametara, mernih podataka i jedinica za izražavanje rezultata merenja, koji uobičajeno podrazumeva procese **evaluacije** (*auditing*, analiza ranjivosti, testiranje na proboj) i/ili **monitoringa** performansi servisa zaštite (tehnički sistem metrike, log datoteke). Metrički sistemi u oblasti zaštite informacija su brojni, a u praksi zaštite najčešće se primenjuju: snaga kriptografskog algoritma; kvalitativna metrika (npr. uticaja: *nizak, srednji, visok*); kvantitativna metrika (*cost - benefit*); metrika softverskog inženjerstva (*SwE*), [5, 8]; detekcija anomalija (IDS/IPS); srednje vreme napada; intervju; metrika poslovnih procesa; metrika kontrole sistema zaštite (*auditing*) i *SSE-CMM* metrika sazrevanja procesa zaštite.

Objekti merenja u sistemu zaštite informacija mogu biti: **organizacija**; **proizvod** (planiran, u razvoju, u radu); **tehnički sistem** (hardver, softver, komunikaciona infrastruktura, komponente sistema zaštite, sistem zaštite u celini).

1.2. Principi, namena i proces metričkog sistema

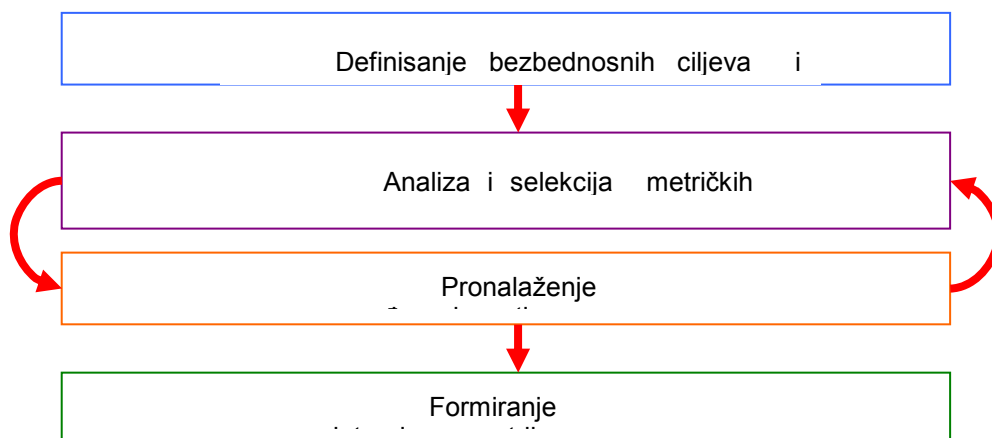
Glavni principi metričkog sistema zaštite su: obezbeđene informacije koje se mogu kvantifikovati (procenti, srednje vrednosti, gradacije 1-3, 1-5, 1-10); uvek dostupni podaci koji podržavaju metrički sistem; samo ponovljivi procesi mogu se smatrati merljivim; upotrebljivost za praćenje performansi sistema zaštite i usmeravanje resursa.

Namena metričkog sistema zaštite je da identifikuje uzroke slabih performansi sistema zaštite (servisa i mehanizama) i omogući odgovarajuće korektivne akcije. Moguće je razviti **tri tipa metričkih sistema** zaštiti, za merenje:

1. *kvaliteta implementacije politika zaštite*;
2. *efektivnosti i efikasnosti servisa zaštite*;
3. *uticaja bezbednosno relevantnih događaja na poslove i misiju organizacije*.

Efektivnost svakog tipa metričkog sistema zavisi od zrelosti programa zaštite organizacije i kvaliteta implementacije kontrola zaštite IKT sistema. Iako se sva tri tipa metričkih sistema mogu koristiti simultano, sa povećanjem zrelosti implementacije kontrola zaštite, primarni fokus se pomera od prvog do trećeg tipa metričkog sistema.

Generički tok procesa metričkog sistema zaštite informacija (Sl. 1.2) u prvom koraku definiše ciljeve zaštite i njihove međuzavisnosti. Zatim se vrši analiza i izbor komponenti metričkog sistema. U sledećem koraku pronalaze se međuzavisnosti i eventualno povratno koriguje izbor komponenti metričkog sistema. Izlazni metrički sistem je složen i kombinovan od više reprezentativnih metrika iz prethodnih koraka, [10].



Sl. 1.2. Generički tok procesa metrike zaštite

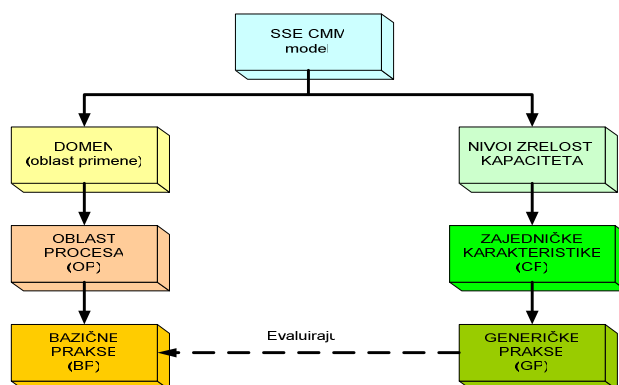
1.3. Metrički sistem procesa zaštite

U procesnom pristupu zaštiti informacija, metrički sistemi mogu meriti organizacione procese (*kontrole*) zaštite, kvalitet proizvoda, performanse tehničkih sistema i dr., a od posebnog značaja su metrički sistemi za merenje sazrevanja procesa zaštite. Razvijeno je više metrika za merenje zrelosti procesa zaštite i upravljanje programom zaštite informacija, kao što su: *SSE-CMM*¹ (*ISO/IEC 21827; EOS, 2001*), *INFOSEC IA-CMM*, *IS Program Maturity Grid* i *SW Security Metrics*, [5].

SSE-CMM međunarodni i evropski standard od 2001 godine, koji meri i određuje zrelost i poboljšanje procesa i kapaciteta zaštite, verovatno je najkompletniji i najlakši za primenu od gore pomenutih metričkih sistema procesa zaštite. Model sadrži dve celine: oblast primene procesa (*Domain side*) i oblast kapaciteta zaštite (*Capability side*), [4], [6]. Oblast primene obuhvata 60 osnovnih praksi zaštite (**BP-Basic Prctices**), koje se obavezno izvršavaju, grupisanih u 11 **tehničkih oblasti procesa** -(**OP**) zaštite 11 **upravljačkih** (projektnih) i **organizacionih** OP zaštite. Oblast kapaciteta modela sadrži tri kategorije: **generičke radnje** (**Generic Practices**)-**GPs** (ukupno 30), koje evaluiraju izvršavanje BP, a grupišu se u **zajedničke karakteristike** (**Common Features**)-**CFs** (ukupno 12), raspoređene na 5 **nivoa zrelosti kapaciteta** (**Capability Levels**)-**CLs**, (Sl.1.1), [1]. Da bi se merio progres efektivnosti implementacije kontrola zaštite, SSE CMM model obezbeđuje 5 nivoa efektivnosti za svaki odgovor na kontrolna pitanja, [6]:

- **0.nivo** – bez aktivnosti i izvršenih procesa zaštite (obično se u modelu izostavlja).
- **1.nivo** – nekompletan, dokumentovan i neformalno izvršavan, postoji politika zaštite
- **2.nivo** – kompletiran i dokumentovan, postoje detaljne procedure
- **3.nivo** – dobro definisan, implementirane i dokumentovane procedure,
- **4.nivo** – kvantitativno meren, verifikovan i kontrolisan, testiranje usaglašenosti sa politikom zaštite i efektivnosti procedura;
- **5.nivo** – najviši, kontinualno poboljšavan, potpuno implementirane i integrisane politike i procedure zaštite u dnevne operacije u celom IKT sistemu organizacije;

Metrika zrelosti procesa zahteva brojne aktivnosti: prikupljanje dokaza o izvršenim praktičnim aktivnostima, korišćenje resursa organizacije, analizu aktivnosti internih ugovarača u odnosu na snabdevače, primenu metoda merenja, tačnost, ponovljivost i nezavisnost procesa, [6].



¹ SSE CMM – Security System Engineering Capability Maturity Mode

Sl. 1.1. Struktura SSE CMM modela i metoda

Za kvalitetno merenje progresivnog sazrevanja procesa treba definisati skup mernih atributa, za: neprekidno inoviranje/optimizaciju procesa; kvantitativno merenje procesa i nastalog proizvoda; praćenje standardnih procesa organizacije; obezbeđenje podrške organizacije (politike, procedure, obuka); planiranje i upravljanje procesima; izvršavanje svih ključnih procesa; izvršavanje nekih delova procesa.

Merenje OP za razvoj programa zaštite, obezbeđuje alat razvijen u *SSE CMM* za merenje SSE, organizacionih i upravljačkih procesa sistema zaštite. Pošto je SSE CMM zasnovan na procesima, a orijentisan na oblast zaštite informacija, metrički sistem treba da obuhvati *dva aspekta*:

1. **Specifičnu metriku procesa**, orijentisanu na same procese, koja se može definisati sa:
 - kvantitativno/kvalitativnim dokazima o nivoima zrelosti SSE OP, ili
 - binarnom indikacijom prisustva/odsustva zrelog procesa.
2. **Metriku sistema zaštite**, orijentisanu na rezultate izvršavanja procesa zaštite, koja:
 - obezbeđuje attribute merenja (objektivne/subjektivne, kvalitativne/kvantitativne) rezultata SSE procesa, koji mogu poslužiti kao dokaz efektivnosti tog procesa.

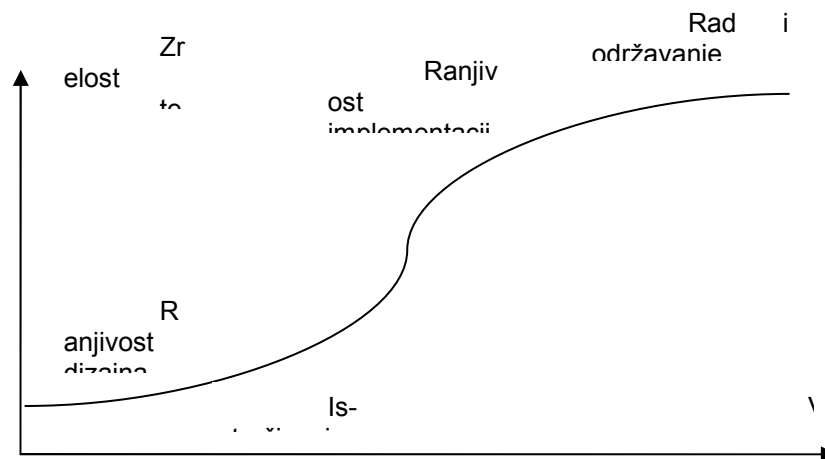
Opšta procedura metričkog sistema zrelosti i sazrevanja kapaciteta procesa za razvoj programa zaštite obuhvata sledeće glavne aktivnosti, [10]:

1. Na svakom nivou (1-5) modela ponderisati sve izabrane *OP* težinskim faktorima od 1-5 koji pozicioniraju datu *OP* na odgovarajući nivo zrelosti (npr. sve *OP* =3 nalaze se na 3. nivou zrelosti, sve *OP*=1, na 1. nivou zrelosti i.t.d.).
2. Na svakom nivou izračunati ukupan zbir težinskih faktora svih *OP*, koji pokazuje nivo zrelosti na datom nivou SSE CMM razvoja programa/procesa zaštite.
3. Razlika između zbira težinskih faktora zrelosti *OP* na višem nivou u odnosu na niži nivo, pokazuje kvantitativnu meru progresivnog razvoja „zrelosti“ procesa i kapaciteta programa zaštite na višem nivou.
4. Izradom osnovnog (referentnog) profila zrelosti procesa/programa na željenom nivou, primenom opšte procedure merenja i profila sazrevanja procesa, posle određenog vremena meri se tekući profil i određuju razlike zrelosti svake *OP* ili zbira *OP* na odgovarajućem nivou kapaciteta u referentnom i tekućem profilu, koje indiciraju nivo progresivnog sazrevanja svakog pojedinačnog/zbirnog *OP*.

U procesu merenja sazrevanja procesa i kapaciteta zaštite i progressa u razvoju programa zaštite treba imati na umu da neke *OP* nije moguće primeniti (odnosno, ciljevi mogu uticati na procenu *OP*) i da je neke *OP* teže izvršiti (odnosno, uniformni cilj je nerealan).

U **Prilogu 1** dat je primer primene metrike modela sazrevanja procesa na bazi koncepta upitnika za samo-procenu (merenje) kontrola *personalne zaštite* i *autentifikacije* u IKT sistemu hipotetičke državne ustanove, [11].

Proizvodi zaštite kao objekti merenja, ranjivi su u fazi razvoja, implementacije i održavanja, zavisno od zrelosti primenjene tehnologije, koja se vremenski menja i stabilise u fazi održavanja (sl. 1.2), pa se merenja mogu vršiti u svim tačkama ranjivosti, [8].



Sl. 1.2. Zrelost proizvoda zaštite

Tehnički metrički sistemi mogu se primeniti u više slučajeva, na primer u: **uspostavljanju cilja zaštite** - za merenje stepena dostizanja postavljenog cilja; **planiranju nivoa zaštite** - za predviđanje nivoa zaštite pre implementacije; **implementiranom sistemu** - za merenje nivoa mogućeg upada (korišćenjem IPS sistema); **usklađivanju** - za upoređivanje nivoa zaštićenosti objekata sistema zaštite u procesu evaluacije ili merenja usklađenosti sa standardom i politikom zaštite; **nadzoru** - za monitorisanje ili skeniranje nivoa zaštite nekog objekta (npr. IDS) i u **analizi** - u slučaju primene metričkog sistema kao metoda za izbacivanje grešaka. **Primeri** tehničkih alata za merenje nivoa zaštite: **IDS/IPS** sistemi; skeneri za monitoring mrežne zaštite; antivirusni programi; antišpijunski i antispam programi, mrežne barijere (*firewalls*) i dr. Svi ovi uređaji generišu određene merne podatke (rezultate merenja) koji se smeštaju u log datoteke tehničkih parametara zaštite. Trend razvoja tehničkih metričkih sistema zaštite je merenje iza IDS/IPS sistema.

Definisanje ciljeva zaštite smatra se ključnom aktivnosti u sistemskom inženjerstvu zaštite (**SSE**), višestruko značajnom: *generalno, u državnim institucijama i industrijskom sektoru* (Tabela T.1.1), [2].

Državne institucije	Industrijski sektor	Generalno
Izgradnja i održavanje poverenja korisnika	Integrisanje rada IKT sistema u poslovne procese	Razvoj svesti o potrebi zaštite IKT sistema
Obezbeđivanje funkcionisanja kritičnih procesa	Bekapovanje poslovne strategije	
Obezbeđivanje harmonizacije glavnih zadataka i normativa	Obezbeđivanje zaštite proizvoda	

T. 1.1. Značaj definisanja bezbednosnih ciljeva za različite potrebe

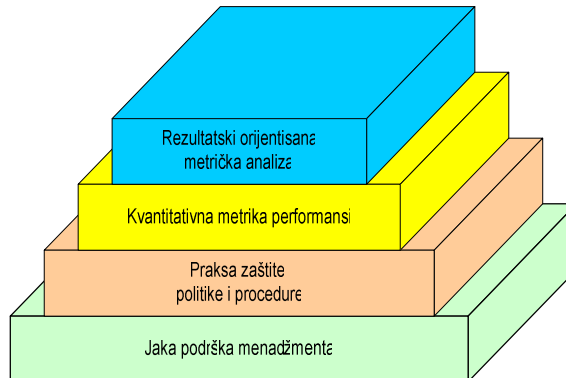
Analiza intervjua podrazumeva izradu *kontrolnih upitnika* za intervjue o zaštiti informacija, u kojima se skupljaju, analiziraju i interpretiraju rezultati razgovora (anketa). Prema iskustvu, upitnici mogu sadržavati 7-8 tema sa ukupno oko 20 pitanja. Intervjuisane organizacije moraju biti raznovrsne (industrijske, državne). Rezultati se analiziraju korišćenjem metoda interpretacije analize, a pokazuju inicijalnu sliku stvarne situacije. Broj uzoraka merenja - izabranih entiteta za intervjue, treba biti prilično velik da bi se rezultati mogli uopštavati. Oblasti za prikupljanje informacija putem kontrolnog upitnika odnose se na **kritične elemente**, a mogu obuhvatiti, [7]: **upravljačke kontrole** (*upravljanje rizikom, revizija kontrola zaštite, razvoj životnog ciklusa sistema zaštite, sertifikacija i akreditacija, planiranje sistema zaštite*), **operativne kontrole** (*personalna zaštita, fizička zaštita, kontrole*

efektivnosti ulazno/izlaznih performansi, planiranje vanrednog događaja, upravljanje konfiguracijom sistema, integritet podataka i sistema, dokumentacija zaštite, svest o potrebi i obuka o zaštiti, upravljanje kompjuterskim incidentom) i **tehničke kontrole** (identifikacija i autentifikacija, logička kontrola pristupa, kontrola log datoteka bezbednosnih događaja). Teme za razgovore mogu biti: okvir sistema zaštite (organizacija, okruženje); bezbednosni ciljevi (iz programa i politike zaštite); metrički sistemi u IKT sistemu; implementacija metričkih sistema; osnove za metričke sisteme (standardi i druga dokumentacija); upravljanje rizikom i kvalitetom zaštite; potreba za metričkim sistemom zaštite (okvir, razvoj).

2. RAZVOJ PROGRAMA METRIČKOG SISTEMA ZAŠTITE

2.1. Struktura programa metričkog sistema zaštite

Program metričkog sistema zaštite treba da uključi 4 interaktivne komponente (SI.1), [10]. Jaka podrška menadžmenta kritična je komponenta za uspeh programa zaštite i implementaciju programa metričkog sistema zaštite. Praktične politike i procedure zaštite, neophodne su za nametanje usaglašenosti, ako ih podržavaju menadžeri. Metrika se ne može lako izvesti, ako nema implementiranih procedura. Kvantitativna metrike performansi sistema zaštite, dizajnira se da obezbedi relevantne podatke o izvršavanju ciljeva zaštite. Mora biti bazirana na izvršavanju ciljeva zaštite, lako dostupna i izvodljiva za merenje, ponovljiva i pogodna za praćenje performansi i usmeravanje resursa zaštite.



SI. 1. Struktura programa metričkog sistema IKT zaštite

Uspeh implementacije programa zaštite procenjuje se u odnosu na stepen proizvodnje relevantnih rezultata, pa program zaštite treba da definiše, [1]: uloge i odgovornosti za program sistema kvaliteta zaštite; metrički sistem(e) zaštite, uputstva za merenja sa prednostima i nedostacima i faktorima uspeha programa svakog sistema merenja; metode i procese koji se koriste u razvoju svakog metričkog sistema; faktore uticaja na implementaciju i implementira program metrike i istakne značaj periodične analize mernih podataka za: obuku, poboljšanje efektivnosti procesa zaštite i planiranje kontrola zaštite.

2.2. Izbor tipa metričkog sistema

Zrelost programa zaštite određuje tipove metričkih sistema koji se uspešno mogu razviti i primeniti. Zreo program zaštite normalno implementira brojne mehanizme za praćenje, dokumentovanje i kvantitativnu verifikaciju različitih aspekata performansi sistema zaštite. Što je više podataka na raspolaganju, to je merenje lakše, a raste i mogućnost automatizacije skupljanja podataka za kvantitativno merenje, u zavisnosti od povećanja broja podataka iz automatizovanih izvora u odnosu na humane izvore. Manuelno skupljanje podataka zahteva izradu upitnika i vođenje intervjua i anketa u organizaciji. Korisniji podaci se dobiju od automatizovanih alata za procenu sistema zaštite, tehnika i alata za sertifikaciju baza podataka o kompjuterskim incidentima i izveštajima i drugim izvorima, kao što su rezultati primene SSE CMM modela za merenje zrelosti programa i procesa zaštite.

Izbor tipa metričkog sistema koji se realno može koristiti za poboljšanje performansi sistema zaštite, zavisi od zrelosti implementacije kontrola zaštite, [6], [7], [10]:

1. Tip (3. nivo zrelosti): *procenat sistema* (n.p.r. radnih stanica/servera u LAN) sa odobrenim planovima zaštite; ***procenat sistema*** (n.p.r. radnih stanica/servera u LAN) sa politikama pasvorda i pravima pristupa konfigurisanim u skladu sa bezbednosnim zahtevima u politici zaštite. Kako se sistem progresivno razvija od 1. i 2. nivoa, rezultati ovih merenja moraju biti manji od 100%, što indicira da sistem još nije dostigao 3. nivo zrelosti. Kada merenje implementacije dostigne i ostane 100%, smatra se da su kontrole zaštite potpuno implementirane i da je sistem zaštite dostigao 3. nivo zrelosti.

2. Tip (4. i 5. nivo zrelosti): kada se program zaštite organizacije razvije i podaci o performansama postanu dostupniji, metrički sistem se fokusira na merenje ***efikasnosti*** – blagovremenosti isporuka servisa zaštite i ***efektivnosti sistema zaštite*** – operativnih rezultata performansi implementiranih kontrola zaštite. Ova metrika je alat za validaciju (***sertifikaciju***) efektivnosti kontrola zaštite, opisanih u planu zaštite, u pogledu zaštite objekata IKT sistema. **Na primer**, proračunom procenta pasvorda koji se mogu krekovati u predefinisanoj vremenskoj periodu, merenjem dužine vremena potrebnog za krekovanje pasvorda usaglašenih sa politikom organizacije, vrši se validacija efektivnosti politike zaštite pasvordom u IKT sistemu organizacije.

3. Tip (5. nivo zrelosti): kada su jednom kontrole zaštite integrisane u procese organizacije, procesi postaju samo-regenerativni, a skupljanje mernih podataka potpuno automatizovano, može se meriti uticaj bezbednosno relevantnih događaja na poslove i misiju organizacije, analizom korelacije podataka. **Na primer**, merenje uticaja obuke na sistem zaštite, podrazumeva kvantifikovanje incidenata po tipu (npr. kompromitacije ruta, kompromitacije pasvorda, malicioznog kôda, **DoS** napada) i korelaciju dobijenih podataka sa procentom obučanih korisnika i administratora sistema.

2.3. Proces razvoja i implementacije programa metrike zaštite

Razvoj i implementacija programa metrike zaštite odvija se kroz dva procesa: *razvoj metričkog sistema i implementacija programa metrike zaštite*, [8], [10].

1. Razvoj metričkog sistema obuhvata inicijalni skup metrika i selekciju odgovarajućeg podskupa, a odvija se kroz dve faze: *identifikacija i definisanje* tekućeg programa zaštite (prva 4 koraka) i *razvoj i izbor tipa metričkog sistema*

kontrola zaštite, koji zavisi od nivoa zrelosti procesa u životnom ciklusu (preostala 3 koraka), uključujući razvoj sva tri tipa metričkog sistema. Učestanost skupljanja rezultata svake metrike zavisi od životnog ciklusa samog događaja merenja, na primer: **merenje procenta** kompletiranih ili ažuriranih planova zaštite, treba vršiti najmanje 1 put u 6 meseci, a **merenje pasvorda** koji se mogu krekovati treba vršiti najmanje 1 put mesečno.

2. Implementacija programa metrike zaštite je iterativna operacionalizacija programa metrike kroz 6 koraka, koji kada se potpuno izvrše, obezbeđuju neprekidnost korišćenja metrike zaštite za monitorisanje i poboljšanje performansi kontrola zaštite i merenja odgovarajućeg aspekta sistema IKT zaštite. Iterativna priroda ciklusa obezbeđuje monitorisanje progresa i planiranog uticaja korektivnih akcija na implementaciju kontrola zaštite. Ako korektivne akcije nisu implementirane, ili planirane, ili daju neočekivan efekat, češće merenje performansi obezbeđuje brzu, internu korekciju, čime se smanjuju problemi koji se mogu otkriti u procesima *auditinga* i sertifikacije.

Na uspeh programa metrike zaštite utiču brojni faktori, a posebno stepen: uključivanja specifičnosti organizacione strukture i upravljivosti procesa i podataka u okviru prihvatljivih ograničenja resursa. Da bi se obezbedila validnost mernih podataka, metodi za skupljanje i proces izveštavanja treba da budu standardizovani. Validnost mernih podataka je ugrožena, ako se skupljaju iz baze koju pogađaju incidenti. Načini skupljanja mernih podataka i izveštavanje o rezultatima merenja, moraju biti jasno definisani u programu metrike zaštite. U **Prilogu 2** data je standardna forma dokumenta za detaljan opis metričkog sistema zaštite, [10]. U **Prilogu 3** prikazan je primer primene metrike za ocenu dva kritična elementa *Plana zaštite*.

Program metrike zaštite je od posebnog značaja za procese digitalne forenzike: istragu i prikupljanje digitalnih dokaza, formiranje neoborivog dokaza, dokazivanje i sudsko veštačenje, jer obezbeđuje **ponovljivost** testiranja i merenja digitalnih dokaza po zahtevu pravosudnih organa, što je jedan od ključnih kriterijuma za priznavanje posrednog digitalnog dokaza pred sudom.

3. PREDNOSTI I NEDOSTACI METRIČKIH SISTEMA ZAŠTITE

Prednosti korišćenja metričkog sistema zaštite za organizaciju su brojne: poboljšanje kontrolisane odgovornosti (*accountability*), ukazivanjem na specifične kontrole koje nisu implementirane ili su nekorektno implementirane; merenje svakog aspekta sistema zaštite, kvantifikovanjem i korišćenjem različitih rezultata (analize rizika, testiranja sistema zaštite na proboj, bezbednosnog testiranja i evaluacije sistema zaštite i aktivnosti u zaštiti); izolovanje problema u zaštiti, na bazi mernih podatke za procenu, opravdanje i usmeravanje investicija na oblast zaštite koju treba poboljšati; usklađivanje sa zakonima i regulativama i angažovanje na proaktivnoj zaštiti; opravdanje investiranja u zaštitu, na bazi kvantitativnih mernih podataka; merenje efektivnosti implementiranih kontrola procesa/procedura zaštite i.t.d.

Nedostaci metričkih sistema su poznati. Glavni problem, svakako je merenje uticaja ljudskog faktora na sistem zaštite. Neke organizacije ga prevazilaze angažovanjem nezavisnih eksperata, pa nemaju potrebu za merenjem uticaja ljudskog faktora. Uzroci slabe ili neadekvatne implementacije metričkih sistema, generalno nastaju najčešće zbog nedostatka ili nepostojanja: jasno definisanih procesa metričkih sistema; svesti o potrebi kvalitetnog upravljanjem zaštitom informacija; spremnosti menadžerske strukture za angažovanje u oblasti zaštite; dokumenata zaštite (*Uputstvo za metriku zaštite*); odgovornosti za sistem zaštite i brojnih tehničkih rešenja metričkih sistema zaštite, [10].

4. ZAKLJUČAK

Metrički sistemi zaštite imaju brojne aplikacije, od monitoringa do procesa analize. Ne postoje široko prihvaćeni i korišćeni standardi za merenje zaštićenosti. U oblasti zaštite daju najbolje rezultate kada se primenjuju kao proces, planiran u pripremnoj fazi razvoja sistema zaštite. Sa aspekta sistema kvaliteta programa zaštite od presudnog značaja je razviti, uspostaviti i implementirati na nivou organizacije program metrike zaštite, razviti metrički sistem zaštite, definisati proces implementacije i model ciklične evaluacije procesa zaštite (SSE-CMM), umesto manje-više slučajnog izvršavanja procesa zaštite.

Proces razvoja metričkog sistema odvija se u dve faze (7 koraka), a proces implementacije metričkog sistema kroz 6 iterativnih koraka, koji kada se potpuno izvrše, obezbeđuju neprekidnost korišćenja metrike zaštite za monitorisanje i poboljšanje performansi kontrola zaštite i merenja odgovarajućeg aspekta sistema IKT zaštite.

Metrika zaštite je od posebnog značaja za procese digitalne forenzike: istragu i prikupljanje digitalnih dokaza, dokazivanja i sudsko veštačenje, pošto obezbeđuje **ponovljivost** testiranja i merenja digitalnih dokaza po zahtevu pravosudnih organa, što je jedan od ključnih standardnih kriterijuma za priznavanje posrednog digitalnog dokaza pred sudom.

5. LITERATURA

1. Bate R., and all, *A Systems Engineering Capability Maturity Model V.1.1*, Software Engineering Institute, US DoD, 1995.
2. Grance T., &all, *Guide to Information Technology Security Services*, NIST SP 800 35, <http://csrc.nist.gov/publications/nistpubs/800-35/sp800-35.pdf>, 2003.
3. Grance T., Hash J., Stevens M., *Security Considerations in the Information System Development Life Cycle*, NIST SP 800-64, <http://csrc.nist.gov/publications/nistpubs/800-64/sp800-64.pdf>, juni 2004.
4. Jeffrey R. W., Karen M. F., *P³I – Protection Profile Process Improvement*, Arca Systems, Inc., william@arca.com, ferraiolo@arca.com, 2004.
5. Pankaj Goyal, *CS497 – Security engineering and software engineering*, Indian Institute of technology, Kanpur, India, e-mail: [pankajgo]@cse.iitk.ac.in, 2005.
6. Petrović R.S., Čekerevac Z., Grubor G., *Security System Engineering Capability Maturity Model in The ICT Security*, 10. međunarodna naučna konferencija “Rešavanje kriznih situacija u specifičnim prostorima”, Fakultet specijalnog inženjerstva, ŽU, Žilina, Slovačka, 2005.
7. Ross R., Katzke S., NIST SP 800-53, A, B, C, *Recommended Security Controls for Federal IS*, <http://csrc.nist.gov/publications/nistpubs/800-53/sp800-53.pdf>, 2005.
8. Savola Reijo, *Measurement of Security in Processes and Products*, www.vitt.ele, 7.04.2005.
9. Stoneburner G., Hayden C. and Feringa A., *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, NIST SP 800-27, <http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf>, 2004.
10. Swanson M., & all, *Security Metrics Guide for Information Technology Systems*, NIST SP 800-55, <http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf>, 2003.
11. Swanson M., *Security Self-Assessment Guide for Information Technology Systems*, NIST SP 800-26, <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>, 2001.

Prilog 1.

Category of Sensitivity	Confidentiality	Integrity	Availability
High	X		
Medium			
Low		X	X

	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made
Specific Control Objectives						
Personnel Security						
Are all positions reviewed for sensitivity level?	X	X	X			
Is appropriate background screening for assigned positions completed prior to granting access?	X	X				X
Are there conditions for allowing system access prior to completion of screening?	X	X				
Are sensitive functions divided among different individuals?	X	X	X			
Are mechanisms in place for holding users responsible for their actions?	X	X				
Are termination procedures established?	X	X				
Authentication						
Are passwords, tokens, or biometrics used?	X	X	X			
Do passwords contain alpha numeric, upper/lower case, and special characters?	X	X				
Are passwords changed at least every ninety days or earlier if needed?	X	X				
Is there guidance for handling lost and compromised passwords?	X	X				
Are passwords transmitted and stored with one-way encryption?	X	X				
Is there a limit to the number of invalid access attempts that may occur for a given user?	X	X				

Prilog 2.

Formular datalnog opisa metričkog sistema

Strateški cilj performanse zaštite	Naveći željene rezultate implementacije jedne ili nekoliko posebnih ciljeva/tehnika kontrola zaštite koje se mere metrikom. To mogu biti kritični elementi (NIST 800-26)
Taktički ciljevi performansi zaštite	Naveći akcije koje se zahtevaju da se postigne opšti cilj performanse zaštite. (Pitanja u NIS 800-26). Više posebnih ciljeva performansi može odgovarati jednom opštem cilju performanse zaštite.
Metrika	Definiši metriku opisujući kvantitativno merenje koje metrika obezbeđuje. Koristi numeričke izraze: „procenat“, „broj“, „učestalost“, „srednja vrednost“, ili drugi sličan termin.
Namena	Opiši sve funkcionalnosti dobijene skupljanjem mernih podataka. Navedi da li se metrika koristi za internu svrhu ili eksterno izveštavanje, kakav uvid u sistem zaštite se očekuje od metrike; legalni ili regulatorni zahtevi za skupljanje specifičnih metrika ako takva postoji.
Dokaz o implementaciji	Navedi listu dokaza o postojanju kontrola zaštite koji vrednuju implementaciju. Dokaz o implementaciji koristi se za računanje metrike, kao indirektni indikator koji vrednuje da su aktivnosti izvršene i kao uzročni faktori koji mogu ukazati na uzroke ne-zadovoljavajućih rezultata za specifično merenje. Poglavlja 4.1.3., 4.1.4., i 4.1.5, ukazuju na informacije koje se mogu koristiti za identifikovanje odgovarajućeg dokaza o implementaciji. Poglavlje 5.2. sadrži listu opštih uzročnih faktora (NIST 800-26).
Formula	Opiši proračun kojeg treba izvršiti da se dobije numerički izraz metrike. Lista dokaza o implementaciji je ulaz u formulu za računanje metrike (procenat, srednja vrednost, verovatnost i.t.d.)
Izvor podataka	Nabroj lokacije podataka koje treba koristiti za računanje metrike. Uključi bazu podataka, alate za praćenje, organizacije ili specifične uloge u organizaciji koje mogu obezbediti potrebne informacije (poglavlje 3.4.3.)
Indikatori	Obezbedi informacije o značenju metrike i trendu njenih performansi. Predloži mogući kurs trendova identifikovanih kroz merenje i ukaži na moguća rešenja za korigovanje uočenih nedostataka. Navedi cilj performanse, ako je postavljen za metriku i indiciraj pozitivan trend za dostizanje tog cilja. (Poglavlje 4.2. Uspostavljanje ciljeva performansi sistema zaštite) . Opiši kako informacije skupljene kroz listu dokaza o implementaciji treba da se koriste kao ulazi u analizu indikatora. Dokazi o implementaciji služe za vrednovanje performansi zaštite i ukazivanje na uzročne faktore.

Prilog 3.

Metrika *Plana zaštite IKT sistema*

Kritični elemenat	5.1. Da li je <i>Plan zaštite</i> dokumentovan za IKT sistem i sve umrežene sisteme?
Potpitanje	5.1.1. Da li je <i>Plan zaštite</i> odobren od strane ključnih zainteresovanih strana i menadžmenta?
Metrika	Procenat IKT sistema sa odobrenim <i>Planovima zaštite</i> .
Namena	Da se izmeri stepen do kojeg su planovi zaštite odobreni od strane menadžmenta, što implicira da su planovi kompletirani i usaglašeni sa primenljivim zahtevima (zakona, standarda, regulativa).
Dokaz implementaciji	o 1. Da li organizacija održava tekući spisak inventara IKT sistema? DA NE 2. Ako DA, koliko sistema u organizaciji postoji? ----- 3. U koliko sistema su kompletirani planovi zaštite? ----- 4. U koliko sistema planovi zaštite sadrže sve standardne strukturne komponente? ----- 5. Koliko sistema ima odobrene planove zaštite od strane menadžmenta? ---
Učestanost	Godišnje
Formula	Broj odobrenih planova zaštite (pitanje 5)/ukupan broj IKT sistema.
Izvor podataka	Spisk inventara i dokumentacija IKT sistema (pitanje 2).
Indikatori	Cilj ove metrike je 100%. Poželjan je trend približavanja nivou od 100%. Kompletiranje plana zaštite zahteva se <i>Zakonom o zaštiti podataka i informacija u IKT sistemima</i> (ako postoji) i <i>ddrugim normativnim aktima i standardima</i> (nabrojati!). Plan zaštite IKT sistema treba potpuno da identifikuje i opiše instalirane ili planirane kontrole zaštite za sistem i treba da sadrži spisak pravila ponašanja. Odobrenje sistema od strane menadžmenta indicira da su zahtevani strukturni elementi adekvatnog plana zaštite kompletirani i usmeravaju odgovarajuću zaštitu sistema.

Komentar: Pitanja 3 i 4 ocenjuju vrednost kompletiranja proхватljivog plana zaštite IKT sistema. Pored toga mogu ukazati na nedostatak obuke menadžmenta ako broj odobrenih planova zaštite od strane menadžmenta premašuje broj planova zaštite koji sadrže sve elemente koje zahteva standardna struktura plana zaštite.

Kritični elemenat	5.2. Da li se <i>Plan zaštite</i> održava ažurnim?
Potpitanje	5.2.1. Da li se plan periodično revidira i prilagođava da odražava tekuće uslove i rizike?
Metrika	Procenat tekućih <i>Planova zaštite</i> IKT sistema.
Namena	Da se odredi ažurnost planova zaštite i uveri da se revidiraju periodično i da su ažurni kako se zahteva.
Dokaz implementaciji	o 1. Koliko sistema ima u vašoj organizaciji? ----- 2. U koliko sistema su kompletirani planovi zaštite? ----- 3. U izveštajnom periodu koliko je planova zaštite revidirano i ažurirano (ako je bilo potrebno) u sledećim vremenskim periodima? (izabraati najbliži vremenski period za svaki sistem; računati planove smo u jednom vremenskom periodu): - u 6 meseci ----- - u 6-12 meseci ----- u 1.2 godine -----
Učestanost	Godišnje
Formula	Ukupan broj revidiranih i ažuriranih planova zaštite (ako je potrebno) u svakom vremenskom periodu (pitanje 3)/ukupan broj kompletiranih planova zaštite (pitanje 2).
Izvor podataka	Spisk inventara koji uključuje sve sisteme za glavne aplikacije i opštu podršku, uputstvo za samo-procenu (NIST SP 800-26) i dokumentacija IKT sistema.
Indikatori	Svaka organizacija treba da postavi ciljni vremenski period za godišnju reviziju i ažuriranje plana zaštite. Broj revidiranih i ažuriranih planova za

svaki vremenski period treba sabrati i podeliti sa ukupnim brojem planova zaštite. Ovaj proračun treba da zadovolji 100% od zahtevanih. Ako cilj nije postignut u okviru vremenskog perioda procenat treba da se približava 100%. Validnost kompletiranih planova zaštite potvrđuje se skupljenim podacima iz metrike 5.1.
--

Komentar: Ova metrika može biti proširena dodavanjem pitanja, na koja bi odgovori mogli pokazati razloge zašto neki planovi zaštite nisu revidirani i odobreni kako se to zahteva.