



**UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE**

**MASTER STUDIJSKI PROGRAM
SAVREMENE INFORMACIONE TEHNOLOGIJE**

SABSA matrica na primeru bezbednosne arhitekture IKT centralne banke

Master rad

Mentor:

Prof.dr Mladen Veinović

Student:

Neda Jerković

Beograd, 2015.

Sadržaj

1. Metodologija istraživanja.....	5
1.1. Predmet istraživanja.....	5
1.2. Značaj istraživanja	5
1.3. Cilj istraživanja	5
1.4. Hipoteze istraživanja.....	6
1.5. Metode i tehnike istraživanja	6
1.6. Struktura rada.....	6
2. Arhitektura bezbednosti i uloga SABSA	8
3. Kontekstualna bezbednost.....	14
3.1. Kontekstualna bezbednost – Imovina	14
3.2. Kontekstualna bezbednost – Motivacija	16
3.3. Kontekstualna bezbednost – Proces.....	17
3.4. Kontekstualna bezbednost – Ljudi.....	18
3.5. Kontekstualna bezbednost – Lokacija.....	19
3.6. Kontekstualna bezbednost – Vreme.....	20
4. Konceptualna bezbednost	21
4.1. Konceptualna bezbednost – Imovina	21
4.2. Konceptualna bezbednost – Motivacija	23
4.3. Konceptualna bezbednost – Proces.....	24
4.4. Konceptualna bezbednost – Ljudi.....	25
4.5. Konceptualna bezbednost – Lokacija	26
4.6. Konceptualna bezbednost – Vreme.....	27
5. Logička bezbednost	28
5.1. Logička bezbednost – Imovina	28
5.2. Logička bezbednost – Motivacija	29
5.3. Logička bezbednost – Proces	30
5.4. Logička bezbednost – Ljudi.....	31
5.5. Logička bezbednost – Lokacija.....	31
5.6. Logička bezbednost – Vreme.....	33

6.	Fizička bezbednost.....	34
6.1.	Fizička bezbednost – Imovina.....	34
6.2.	Fizička bezbednost – Motivacija.....	36
6.3.	Fizička bezbednost – Proces	37
6.4.	Fizička bezbednost – Ljudi	38
6.5.	Fizička bezbednost – Lokacija	39
6.6.	Fizička bezbednost – Vreme	40
7.	Komponente bezbednosti.....	41
7.1.	Komponente bezbednosti – Imovina.....	41
7.2.	Komponente bezbednosti – Motivacija.....	42
7.3.	Komponente bezbednosti – Proces	43
7.4.	Komponente bezbednosti – Ljudi	43
7.5.	Komponente bezbednosti – Lokacija.....	44
7.6.	Komponente bezbednosti – Vreme	44
8.	Operativno upravljanje bezbednošću	45
8.1.	Operativna bezbednost – Imovina.....	46
8.2.	Operativna bezbednost – Motivacija.....	47
8.3.	Operativna bezbednost – Proces	48
8.4.	Operativna bezbednost – Ljudi	49
8.5.	Operativna bezbednost – Lokacija.....	49
8.6.	Operativna bezbednost – Vreme	50
8.7.	Operativna bezbednost kroz sve slojeve matrice	51
9.	Vertikalni slojevi SABSA matrice.....	53
10.	Zaključak.....	53
	Opis skraćenica	55
	Literatura:.....	56
	SABSA Matrica razvoja bezbednosne arhitekture	57

1. Metodologija istraživanja

1.1. Predmet istraživanja

Predmet rada je analiza implementacije arhitekture bezbednosti u finansijsku instituciju, u ovom slučaju centralnu banku, odnosno njen deo (Sektor za informacione tehnologije) prema SABSA metodi.

1.2. Značaj istraživanja

Značaj ovog rada je u doprinosu dokumentovanosti SABSA metode na srpskom jeziku, posebno u analizi postupaka korak po korak kroz SABSA matricu. Rad daje praktična i konkretna uputstva kako, prateći matricu, doći do upotrebljive osnove za stabilnu i dokumentovanu bezbednosnu arhitekturu. Poseban značaj je što rad pokazuje da se ova metoda može koristiti i u celoj organizaciji, ali i primeniti na jedan njen deo. Ovde je upravo opisano kako se bezbednosna arhitektura implementira najpre u IT sektoru, što je dobra metodologija za velike organizacije koje nemaju uspostavljene procese upravljanja rizikom i kontinuitetom poslovanja, a traže da se implementira zaštita informacionih sistema. Budući da je prateća dokumentacija često najveći problem prilikom uvođenja bilo kakvog sistema, u radu je dat predlog i za prateću dokumentaciju, sa osnovnim elementima, kao i načini da se izbegne dupliciranje repozitorijuma tako što će se u dokumentaciji referencirati na postojeće evidencije ugrađene u aktuelnu poslovnu i infrastrukturnu arhitekturu. Pritom se neretko pokazuju manjkavosti postojećih repozitorijuma i motiviše njihovo poboljšanje.

1.3. Cilj istraživanja

Naučni cilj istraživanja je da se praktično proveriti naučna vrednost i primeni teorija SABSA metode u konkretnom okruženju, bezbednosnim zahtevima i ostalim specifičnim uslovima.

Društveni ciljevi istraživanja uključuju više aspekata:

1. Prvi cilj istraživanja SABSA metode je prvenstveno pronalaženje jednostavnog i razumljivog postupka za uspostavljanje bezbednosne arhitekture u organizaciji ili nekom njenom delu, praveći pritom stabilan i skalabilan gradivni blok za ukupnu arhitekturu, kako IKT tako i organizacije u celini.
2. Istovremeno, cilj je da se istraži da li je metoda dovoljno fleksibilna da i u slučajevima nedovoljne dokumentovanosti pojedinih tačaka i nepostojanja kontrola zadrži svoju strukturu i služi svrsi.
3. Traži se takođe da se istraži da li se prateći SABSA matricu može doći do informacija o propustima u već postojećoj poslovnoj i infrastrukturnoj arhitekturi, da li postoje redundantni izvori, suvišni procesi, zastarela oprema, servisi koji više nisu u upotrebi i slično. Stavlja se na proveru i postojeća organizacija zaposlenih i interpersonalne veze, kao i kompetencije pojedinih učesnika u poslovnim procesima.

4. Istraživanje treba da, osim predloga bezbednosne infrastrukture, pokaže da li je predložena dokumentacija korisna i u utvrđivanju stanja infrastrukture i servisa, i koji su joj sporedni benefiti i upotrebnost vrednost.

1.4. Hipoteze istraživanja

Opšta hipoteza je da je arhitektura bezbednosti determinisana ostalom arhitekturom, odnosno veličinom organizacije, načinom funkcionisanja, ulaganjima u IKT, kritičnosti IKT funkcija, postojanjem upravljanja rizikom i opredeljenošću rukovodstva da se ona implementira.

Posebne hipoteze koje usmeravaju tok istraživačkog rada su:

1. Da je, usled nepostojanja uslova da se bezbednosna arhitektura implementira u celoj organizaciji, to moguće uraditi i u samo jednom njenom delu, konkretno IKT sektoru.
2. Da posvećenost rukovodstva i opredeljenost da se ulaže u bezbednosne mehanizme predstavlja neophodan uslov da se bezbednosna arhitektura implementira.

1.5. Metode i tehnike istraživanja

Budući da se radi o temi koja je na našem jeziku slabo dokumentovana, metod za prikupljanje opštih informacija je uglavnom konsultovanje strane literature, naučnih i istraživačkih radova. Osnovni metod je, ipak, da se analitički prati SABSA matrica i sledeći korake, sintetički kreira originalan pristup za konkretan slučaj. SABSA okvir daje smernice šta su kontrolne tačke, a gradivni blokovi arhitekture moraju biti autentični. Budući da se radi o specijalnom slučaju implementacije arhitekture bezbednosti samo u jedan deo organizacije, u IKT sektor, to je i metodologija prilagođena praćenju pojava u određenim granicama, ali vodeći računa o uticaju na čitavu organizaciju, jer je upravo specifičnost IKT da podržavaju ostvarivanje poslovnih ciljeva organizacije, a ne delatnost po sebi i za sebe. Kad je u pitanju prateća dokumentacija koju rad daje kao predlog, ona je dizajnirana na osnovu višegodišnjeg iskustva u sistem analizi, projektovanju i dokumentovanju, i ne predstavlja celovito rešenje već samo nacrt rešenja.

Predložena struktura pratećeg dokumenta data je u osnovnim elementima, a sadržaji polja su popunjavani za deo dokumenta i to opštije nego što bi se to radilo u pravoj realizaciji. Svrha popunjavanja je da se objasni ideja, a ne da se prikaže gotova dokumentacija. Zbog specifičnosti organizacije koja se analizira (centralna banka), podaci su uopšteni, ali to ne utiče na izvođenje zaključka, prikaz metodologije i dokazivanje njene upotrebljivosti.

U istraživanju su korišćene opšte logičke metode dedukcije, indukcije i apstrakcije, kao i opšte statističke metode analize, sinteze i generalizacije.

1.6. Struktura rada

Kroz rad će se predstaviti jedna moguća metodologija u implementaciji arhitekture bezbednosti u IKT sektor velike finansijske organizacije sa kompleksnom IKT infrastrukturom, korak po

korak. Pored objašnjenja svakog koraka, dat je i predlog konkretnih podataka za posmatranu organizaciju, ali dovoljno opšte, da se može zaključiti šta je zapravo cilj koraka, i da se može primeniti na bilo koji poslovni sistem odnosno podsistem. Rad sledi SABSA matricu i prema tome je i podeljen u šest glavnih delova koji prate šest slojeva arhitekture, kojima prethodi uvod o arhitekturi uopšte, nakon čega sledi još jedno poglavlje koje daje dodatne informacije o SABSA metodi i oblastima na koje se ona odnosi. Na kraju je zaključak u kom se daju stepen u kom je rad ispunio postavljene hipoteze i ocena doprinosa saznanja do kojih se u radu došlo.

2. Arhitektura bezbednosti i uloga SABSA

Termin *Arhitektura preduzeća* ili organizacije (eng. Enterprise Architecture – EA) nastao je krajem osamdesetih godina prošlog veka, i to prvo kao sistem za modeliranje IKT funkcija, a zatim i celog preduzeća. Osnovni problemi koje je trebao da reši sistemski pristup arhitekturi, bili su sve veća složenost IKT struktura sa jedne strane, i nemogućnost da se IKT funkcijama na odgovarajući način pokriju poslovne funkcije. Arhitektura preduzeća gradi se na preseku poslovne strategije, operativne efikasnosti i tehnološke optimizacije.

U novije vreme sistemi za obradu podataka su postali složeniji, a potreba za deljenjem informacija i njihovom dostupnošću mobilnom korisniku sve veća i danas zapravo govorimo o informaciono-komunikacionim tehnologijama (IKT). Arhitektura preduzeća se dokumentuje i analizira upravo u IKT sektoru preduzeća (organizacije), jer IKT svoju svrhu ima upravo u podršci poslovnoj funkciji i nikako drugačije. Ovo je nešto što se u praksi često izgubi iz vida i zato je postavka arhitekture bitan princip koji usmerava akcije IKT u organizaciji i determiniše strategiju razvoja i rada IKT sektora.

Arhitektura bezbednosti informaciono komunikacionih sistema može da se definiše kao detaljan opis svih aspekata sistema i/ili opreme koji se odnose na bezbednost, a zatim i skup principa i smernica za dizajniranje sistema i/ili opreme, jednako kao i izbor i implementaciju bezbednosnih mera.

Arhitektura bezbednosti predstavlja skup pravila i dogovorenih koraka koji:

- usmerava proces projektovanja i održavanje sistema zaštite,
- odražava potencijalna ograničenja okruženja, resursa, veština zaposlenih i tehnologija
- služi za upravljanje kompleksnošću sistema
- primenjuje principe sistemskog inženjerstva za postizanje poslovnih ciljeva
- obezbeđuje okvir procedura, tehnologija i procesa
- obezbeđuje postojanje i rentabilnu implementaciju, upotrebu i održavanje sistema zaštite

Metodološki pristup arhitekturi bezbednosti ima za cilj da¹ :

- minimizira raznovrsnost tehnologija
- obezbedi konzistentnu funkcionalnost sistema zaštite informacione imovine
- integriše servise i mehanizme zaštite u sistem zaštite
- deli sistem zaštite na različite domene i kontroliše tok informacija između njih
- primenjuje konzistentne metode, tehnike i konvencije u sistemu zaštite

Cilj je da se koncept bezbednosti koliko god je to moguće ugrađuje u inicijalni dizajn sistema i podsistema, a ne da se implementira naknadnom nadogradnjom. Ovakav pristup pruža

¹ G.Grubor: Projektovanje menadžment sistema zaštite informacija, Univerzitet Singidunum, 2012.

moćnost jednostavnijeg prihvatanja novih tehnologija, kao i prelaska na nove platforme i nove poslovne modele. Takođe, ovakva izgradnja arhitekture omogućuje da se analiza troškova odradi tačno i pravovremeno.

Teoretski, izgradnja arhitekture organizacije sadrži u sebi i postavljanje IKT arhitekture, i bezbednosne arhitekture kao njenog sastavnog dela. U praksi, stvari su malo drugačije. Srećemo se sa organizacijama koje već imaju postavljene poslovne modele, gde se informaciono-komunikacione tehnologije posmatraju kao servis koji se prilagođava poslovnim modelima, najčešće na dnevnoj bazi i po ne uvek dobro definisanim pravilima, a bezbednosna arhitektura postoji samo u tragovima, i to kroz (najčešće tehnološka rešenja) bezbednosne mere koje se implementiraju na opšta mesta ili nakon što se nešto dogodi.

Već i samo uočavanje ovog jaza sugerise da je prvi korak izrada neke vrste „gap“ analize, koja će nam pružiti informaciju o tome gde smo i gde želimo da budemo. Predmet ovog rada je to „željeno stanje“, a biće obrađeno kroz standardizovanu SABSA metodologiju, pri tom ne zanemarujući činjenicu da se u većini slučajeva arhitekta bezbednosti susreće sa nekim zatečenim stanjem, pre nego sa određenim rukama i neograničenim budžetom. Međutim to nije prepreka da se postojeća IKT arhitektura dobro objasni, što predstavlja preduslov nadgradnji u vidu arhitekture zaštite.

Osnovni koncepti arhitekture zaštite su: Prstenovi zaštite, slojevitost, apstrakcija i bezbednosni domeni. **Prstenovi** zaštite definišu se po restriktivnosti zaštite od centralnog (kernel OS) prema aplikativnom sloju (OS - OS Utilities - FS Drivers - Clients, processors..). Arhitektura treba da bude i **slojevita**, pri čemu svaki sloj predstavlja različitu perspektivu zaštite i angažuje različite uloge, a gornji sloj usmerava i upravlja donjim slojem zaštite. **Apstrakcija** je koncept pogleda koji krajnji korisnik ima, ne znajući za mehanizme koji se pokreću da bi se servis isporučio, dok su **domeni** zaštite definisani npr. zajedničkim bezbednosnim rizikom, pravima pristupa i slično.

U ovom radu obrađuje se koncept slojevitosti arhitekture bezbednosti IS, i kako se takva slojevitost može primeniti u analizi stanja i implementaciji bezbednosnog okvira u finansijskim organizacijama. Iako su sve bezbednosne arhitekture po svojoj prirodi slojevite (tretiraju bezbednost u kontekstu slojeva mreže, aplikacija, korisnika, platforme i uređaja i rezultuju strategijom „odbrane po dubini“), upravo SABSA metodologija je izabrana iz nekoliko razloga:

- Radi se o metodologiji koja se naslanja na posmatranje IKT bezbednosti kao sredstva u postizanju smanjenja rizika i obezbeđenja kontinuiteta poslovanja
- SABSA je oslonjena na poslovne potrebe i procenjeni rizik, što je za finansijske institucije bolji pristup
- Metodologija je skalabilna i može da se primeni kako na ceo sistem, tako i na delove i podsisteme unutar organizacije
- SABSA je otvoreni standard i nema troškove sertifikacije

- Nema posebna ograničenja za pojedine oblasti industrije i usluga, svuda je jednako primenjiva
- Lako se uklapa sa standardima bezbednosti ISO 27000, kao i upravljanjem servisima i procesima (ITIL, COBIT)
- Lako se uklapa u standardne modele arhitekture kao što su Zahman, i TOGAF
- Kontinuirano se održava i razvija i publikuju se najnovije verzije

Kontekst bezbednosti informacija uvek se posmatra zajedno sa upravljanjem poslovnim rizikom, jer na njega direktno utiče. Zato analiza i upravljanje bezbednošću informacija ne može da egzistira samo za sebe. Uticaj bezbednosti na rizik iskazuje se kroz kategorije koje su zapravo poznate iz definicije bezbednosti, a to su očuvanje poverljivosti, integriteta i dostupnosti informacija. Očuvanje poverljivosti znači da je način pristupa poverljivim informacijama obezbeđen samo ovlašćenim osobama, integritet predstavlja obezbeđenje da informacija nije izmenjena, a dostupnost podrazumeva da informacije uvek budu dostupne kad je to potrebno.

Rizik se procenjuje na osnovu uticaja koji gubici poverljivosti, integriteta i dostupnosti mogu imati na imovinu i poslovanje organizacije. Štaviše, ukoliko organizaciji nedostaju jasne politike bezbednosti i poslovni zahtevi koji iniciraju implementaciju određenih mera, rešenje problema treba tražiti u boljem upravljanju rizicima, a ne u bezbednosnoj arhitekturi.

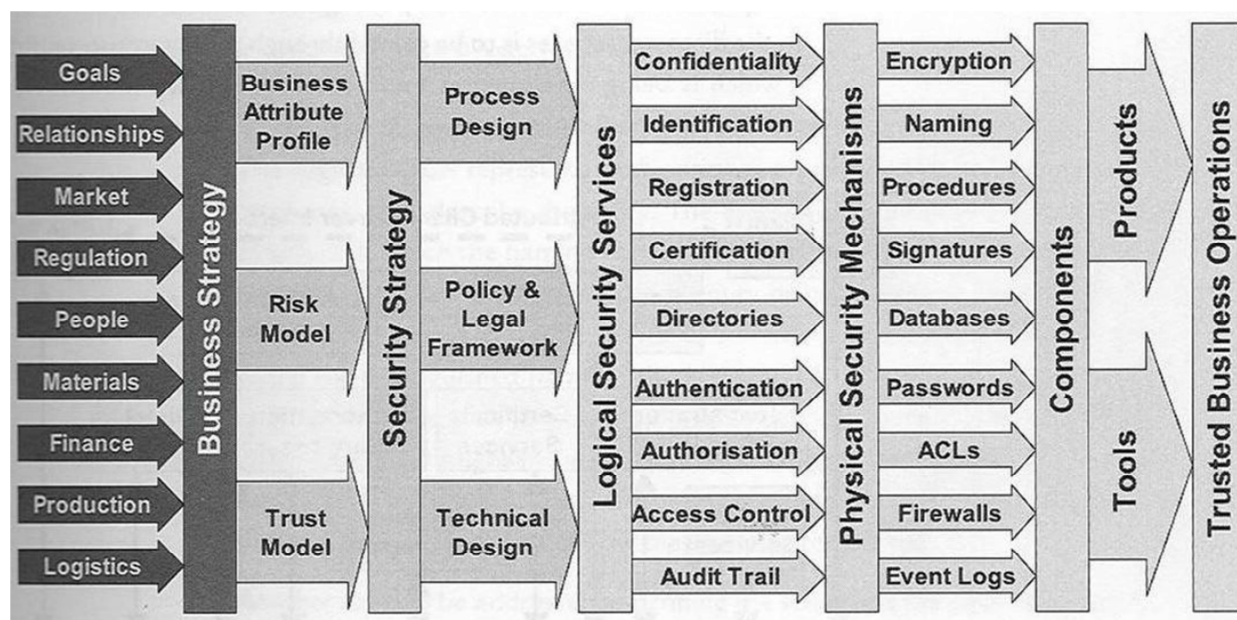
Izazovi koje pred organizaciju postavlja implementacija bezbednosne arhitekture su u prepoznavanju specifičnih potreba i rizika organizacije, nasuprot uniformnoj primeni predefinisane bezbednosne matrice. Problem koji nastaje ukoliko se ne uvažavaju specifičnosti organizacije pri poslovnoj analizi, a zatim i primeni bezbednosnih mera, vode do toga da se funkcija bezbednosti ne tretira sa dovoljno uvažavanja, a ponekad čak doživljava i kao balast. Centralna banka, kao osnovni model uzet u ovom radu interesantna je sa dva stanovišta: nosi rizik finansijske organizacije, ali kao krovna institucija nosi rizik i ukupnog finansijskog sektora. Istovremeno, kao velika organizacija u kojoj se na velikom broju radnih stanica obavljaju različiti poslovi, ne trpi komplikovane, za korisnike i radne stanice zahtevne i usporavajuće metode zaštite.

Da bi se pomirili zahtevi poslovne strane za brzinom i efikasnošću procesa i jednostavnošću interfejsa, sa zahtevima za bezbednost i standardizaciju, organizacijama je vrlo važna uloga poslovnog analitičara [3]. To je stručnjak ili tim koji predstavlja sponu između poslovnih procesa i njihovih zahteva s jedne, i implementiranih tehnoloških rešenja (među kojima su i bezbednosna) sa druge strane. Kad se govori o analizi poslovnih procesa misli se na sagledavanje svih procesa u organizaciji, kao i ciljeva same organizacije, te rizika inherentnih procesima, kao i onih koje nose specifične implementacije. Kada je u pitanju informaciona bezbednost, poslovni analitičar detaljno sagledava aspekte bezbednosti, ali ne gubeći iz vida zahteve poslovnog

procesa ². Nadalje, zadatak poslovnog analitičara je da spreči grešku koju često prave arhitektae prilikom implementacije rešenja, a to je da se samo čekiraju pojedine tehničke i proceduralne kontrole, bez analize njihovih međusobnih relacija i interakcija. Stoga je ideja holističkog pristupa bolja nego lančano čekiranje ispunjenih zahteva [1].

Model kojim se ovde bavimo, SABSA model, upravo je izabran zbog svoje kako sveobuhvatnosti, tako i praktičnosti i fleksibilnosti, jer pomaže da se uoče specifičnosti i pojedini aspekti poslovne analize i bezbednosnih instrumenata. Analiza se bazira na pitanjima na koja treba odgovoriti pre početka dizajniranja rešenja. To su pitanja koja pomažu da se preciznije odabere rešenje i izbegnu skupe greške i nezadovoljstvo korisnika.

Radi se o modelu za postavku bezbednosne arhitekture koji prati sva četiri dela životnog ciklusa informacionih tehnologija: Strategiju, dizajn, implementaciju te upravljanje i održavanje, a sam model je podeljen na šest slojeva [6]. Reč je o metodologiji koja je, kako samo ime kaže, upravljana poslovnim potrebama, a kad se to svede na jezik struke i stavi u kontekst preseka poslovnih zahteva i informacione bezbednosti, vidi se da je to zapravo upravljanje rizikom.



Slika 1a: Proces izrade strategije i dizajna po SABSA [6]

Da bi se osiguralo da su rezultati (postizanje željene arhitekture) konzistentni sa ukupnim poslovnim potrebama, potreban je sistemski pristup [1].

Uloga sistemskog inženjeringa ovde je da obezbedi struktuiran dizajn informacionog sistema unutar realizacije bezbednosne arhitekture. Takva arhitektura treba da

² Česta greška arhitektae bezbednosti je da se fokusira na bezbednost, a da gubi iz vida stvarne potrebe posla, tj. zašto se sve to radi [1]

- Ispuni zahteve koji joj se definišu
- Uspešno se izvršava unutar okruženja (sistema)
- Upravljiva je, sa merljivim performansama

Razvoj ovakve arhitekture pretpostavlja :

- Jasno razumevanje granica sistema koji obezbeđujemo
- Donošenje racionalnih i sledljivih odluka o tome kako će se realizovati
- Uzimanje u obzir svih aspekata sistema u svakom momentu razvojnog procesa, tako da nedostaci mogu biti otkriveni i rešeni uz najmanji uticaj

Razlozi za sistemski pristup su prvenstveno u upravljanju kompleksnošću, dekompoziciji sistema na podsisteme koji su upravljivi (*top-down*), modeliranje procesa (*black-box modelling*) tako da se ne gleda u unutrašnjost procesa već se on posmatra kao crna kutija i analizi logičkog toka, gde svaki izlaz mora predstavljati ulaz u sledeći proces. Na taj način može se uspostaviti željena granulacija, i posmatrati sistem i podsisteme na više nivoa, pri čemu se uvek ima ispred sebe jedan struktuiran okvir unutar koga se razmišlja o sistemu i dizajniraju sistemska rešenja.

Pojednostavljen pogled sa prethodne slike (Slika 1a) na arhitekturu bezbednog okruženja koje može biti upotrebljeno za razvoj poslovnih rešenja za bilo koji nivo detaljnosti i kompleksnosti sistema dat je na **Slici 1b**.



Slika 1b. Slojevita arhitektura bezbednog okruženja

Model ima slojevitú strukturu kao što je prikazano na slici 1b. Svaki sloj sadrži odgovarajuća pitanja definisana iz različitih gledišta.

1. Kontekstualna arhitektura – pogled s nivoa poslovanja
2. Koncept arhitekture zaštite – pogled arhitekta sistema zaštite
3. Logička arhitektura zaštite – pogled projektanta sistema zaštite
4. Fizička arhitektura zaštite – pogled programera/administratora sistema zaštite
5. Komponente arhitekture zaštite – pogled snabdevača
6. Operativna arhitektura zaštite – pogled menadžera

Na svakom od ovih nivoa SABSA model zahteva odgovor na pitanja:

- **Šta?** (Imovina, ono što je predmet zaštite, subjekt pogleda),
- **Zašto?** (Motivacija, zašto to trebamo i šta time želimo postići),
- **Kako?** (Proces, detaljna funkcionalna specifikacija),
- **Ko?** (Ljudi i relacije, kome će to trebati, ko to koristi i na koje načine),
- **Gde?** (Lokacija, geografska pozicija, distribucija, veze, infrastruktura)
- **Kada?** (Vreme, životni ciklusi, period korišćenja, redosled, vremenska agenda)

Dok je prvih pet slojeva relativno nezavisno, operativni sloj arhitekture je donekle poseban, te ga autori predstavljaju na razne načine, kao sloj koji podupire, natkriva ili prožima ostalih pet slojeva. Kad se radi o konkretnim koracima u implementaciji, moglo bi se reći da se operativna arhitektura uključuje negde zajedno sa definisanjem logičke arhitekture (Slika 2).



Slika 2. Proces razvoja arhitekture po SABSA modelu (Izvor: Mark Battersby, Capgemini, 2011)

U radu se detaljno objašnjava logika SABSA pristupa i SABSA matrice (Prilog 1), i objašnjavaju redom slojevi matrice te objašnjavaju međuzavisnosti i veze sa drugim standardima. Istovremeno, kao verifikacija primenjivosti modela, daje se predlog za konkretnu dokumentaciju koja prati postavku arhitekture na studiji slučaja implementacije bezbednosne arhitekture u veliku finansijsku instituciju kao što je centralna banka.

Hipoteza je da se, kad je organizacija previše velika da bi bila fleksibilna, posao implementacije arhitekture bezbednosti može započeti u IT sektoru, čak i za metodologiju kao što je SABSA koja je rukovođena poslovnim ciljevima i poslovnim rizicima.

Uobičajen prikaz SABSA modela je kroz matricu (Prilog1), gde se jasno vidi kretanje i odnosi među fazama, kako vertikalno tako i horizontalno. Opisi koraka pratiće kretanje kroz matricu, uz osvrt na konkretnu izvedbu na primeru jedne velike finansijske institucije sa uspostavljenom i diversifikovanom IKT funkcijom, u ovom slučaju centralne banke. Tako se ujedno i kroz konkretnu dokumentaciju koja predstavlja izlaz iz svakog sloja implementacije bezbednosne arhitekture vrši svojevrsna verifikacija upotrebljivosti samog modela.

3. Kontekstualna bezbednost

Prvi sloj modela SABSA arhitekture, kontekstualna bezbednost, predstavlja pogled sa **nivoa poslovanja**: budući da je poslovno okruženje i poslovni ciljevi zapravo kontekst u koji će se smestiti ili koji će pokriti (oba izraza imaju smisla) bezbednosna arhitektura. Pogled sa nivoa poslovanja obezbeđuje osnovne termine na koje će se naslanjati naredni slojevi. Ovde se imenuju poslovni procesi i poslovni ciljevi, motivacija i rizik, navode se sredstva za dostizanje ciljeva i sve ono čime organizacija raspolaže, a što služi u poslovne svrhe. Sve to ima neposredan uticaj na stvaranje određene, unikatne arhitekture, drugačije od svih ostalih, jer upravo ta arhitektura treba da ispuni očekivanja zaštite i smanjenja rizika tog određenog poslovanja i zato je veoma važno da se elementi konceptualne bezbednosti identifikuju dobro i pažljivo.

3.1. Kontekstualna bezbednost – Imovina

Odgovor na pitanje **šta** je sadržaj pogleda na arhitekturu zaštite sa nivoa poslovanja je: Poslovne funkcije i poslovne odluke, odnosno sve ono što je u službi njihovog ispravnog i pravovremenog donošenja. Poslovne odluke trasiraju poslovanje, a iza njih se krije poznavanje strukture poslovanja, kao i neprestana svest o ciljevima poslovanja.

U ovoj tački projektovanja imenujemo naš posao, navodimo utvrđene ciljeve i zadatke i definišemo sva sredstva koja su potrebna da se dostignu poslovni ciljevi i ispuni svrha. U bezbednosnoj arhitekturi to će zapravo biti sve ono što je predmet zaštite.

Dok je na zapadu prvenstveno zastupljen model kvantitativnog (novčana vrednost) iskazivanja, kako ciljeva tako i pokazatelja i vrednosti, čak i kad se radi o organizacijama koje nisu dominantno profitne (institucije, državna uprava), u okruženju se taj model još uvek ne primenjuje dovoljno, budući da ne postoji ni praksa niti metodologija da se na primer interni servisi izražavaju u ceni koštanja, već se vrednost dodeljuje samo onome što ima realnu tržišnu cenu. S tim u vezi predlog iskazivanja konteksta bezbednosti sadrži deskriptivne odrednice u delu koji se odnosi na opis posla, dok za ciljeve i zadatke, kao i potrebna sredstva može biti primenjen i kvantitativni i kvalitativni prikaz.

Kad je u pitanju povratak investicija - ROI (*Return of investment*), bitno je naglasiti da se u slučaju bezbednosne arhitekture, iako postoji metodologija izračunavanja i odgovarajući prikazi, suočavamo sa velikim teškoćama prilikom argumentovanja potrebe za bezbednosnim mehanizmima pred najvišim rukovodstvom, odnosno donosiocima odluka. U tom slučaju pribegava se izračunavanju potencijalnog gubitka koji bi nastao ukoliko se mere ne bi primenile. Takođe, ukazuje se na kompromise (eng. *trade-offs*), koji se pri tom moraju preduzimati.

Dakle, realizacija ovog koraka u izgradnji bezbednosne arhitekture po SABSA modelu, to jest odgovor na pitanje „šta“ u kontekstu bezbednosti je spisak svih resursa koji omogućavaju organizaciji da dostiže svoje poslovne ciljeve i opravda svoje postojanje. To je ono što se po ISO27002 naziva *informacionim dobrima*, odnosno *informacionom imovinom*, a obuhvata: Ljude sa njihovim znanjima i sposobnostima, informacije u svim oblicima i sistemski i aplikativni softvere (*čista informaciona imovina*), opremu (hardver, mrežnu infrastrukturu, ugrade itd. – *fizička imovina*) i zaposlene, partnere, saradnike (*humana imovina*).

Pretpostavka je da su ovi katalozi urađeni pažljivo i precizno, te da daju informaciju o kompletnoj IKT arhitekturi, ne samo popisanoj u vidu osnovnih sredstava, već kroz performanse i modele svih zastupljenih IKT komponenti.³

Moguće je da će se na ovu fazu potrošiti najviše vremena, pogotovo ako odranije ne postoji dokumentacija koja je definiše. Ako se radi od nule, korisno je da se dokumentacija uradi tako da bude u potpunosti skalabilna, i da se lako proširuje da bi se koristila i u definisanju IKT arhitekture, kao i arhitekture čitave organizacije. Dobro je da se uoči i izbegne redundansa, te da se potrebni podaci o poslovnim ciljevima imovini i procesima nalaze na jednom mestu, makar to značilo veći inicijalni posao, ili dodatni posao oko prepravljanja ranijih verzija.

Dobro dokumentovanje konteksta je značajna osnova za sve dalje aktivnosti, i ukoliko je precizno urađeno ima veliki pozitivan uticaj na pouzdanu, pravovremenu i ispravno lociranu zaštitu kao i optimizaciju troškova. Isto tako, loše definisan kontekst zaštite, sa nedostajućim delovima ili redundansama može uzrokovati propagaciju greške kroz sve ostale slojeve i rezultovati lošim izborom kontrola i njihovom neefikasnošću, kao i povećanjem troškova.

Analizom postojeće dokumentacije i načinima vođenja evidencija u posmatranoj centralnoj banci, uočeno je da se IKT imovina načelno evidentira, ali da postoji još mesta za unapređenje evidencija i optimizaciju. Hardver, softver i konfiguracije dostupni su kroz Service Desk (SD) i Configuration Manager (CM) rešenja, ali ne postoji automatska sinhronizacija, tako da se radi o dve evidencije, pri čemu je SD kompletnija (sadrži sva osnovna sredstva), a CM detaljnija (sadrži podatke o konfiguracijama, ali ne objedinjava različite operativne sisteme). Pored toga, uočeno je da aplikativni portfolio sadrži attribute vezane za osobine aplikacije, lokaciju, fazu

³Poželjno je da se, ako ne ranije, a ono paralelno ovi katalozi urade i za potrebe definisanja kompletne IT arhitekture, te da sadrže detaljan opis korištene opreme (mikroprocesori, memorija, standardi matičnih ploča) kao i konfiguraciju mreže, opise mrežnih uređaja, kao i detaljan aplikativni portfolio.

životnog ciklusa, platformu, ali ne i podatke o procenjenom riziku i kritičnosti (CA – Criticality Assesment), posebnim bezbednosnim zahtevima, značaju za kontinuitet poslovanja.

Takođe, kod evidencije zaposlenih, koja je sa IKT funkcijom povezana putem Identity Manager (IM) rešenja, nisu dovoljno dobro obrađene IKT kompetencije (banka na generalnom nivou poznaje samo kategoriju „poznavanje rada na računaru“, što je za IKT osoblje neprimenjiva kategorija). Radna mesta su opisana kroz zadatke koji se obavljaju, ali su zahtevi u pogledu kompetencija prilično opšti. O konkretnom zaposlenom postoje samo evidencije o završenom školovanju, a od dodatnog obrazovanja samo o onome što je finansirala banka. Sve se to vodi u Ljudskim resursima, a rukovodstvu IKT sektora je dostupno samo na zahtev.

IM i AD rešavaju problem autentifikacije i autorizacije, kao i dodele prava, ali ne i kompetencije.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 1.1.**

3.2. Kontekstualna bezbednost – Motivacija

Ukoliko se sa nivoa poslovanja postavi pitanje: Zašto je potrebna informaciona bezbednost? , očigledno je da odgovor možemo naći samo na jednom mestu: u procenjenom riziku i pretnjama po informacionu imovinu, a time i na ukupno poslovanje. Zapravo čitav ovaj korak bi mogao da se referencira na postojeću dokumentaciju koja je proizašla iz procene rizika i upravljanja rizicima. Organizacije koje nemaju uspostavljeno upravljanje rizikom i identifikovane makar osnovne rizike i kritične procese s jedne, i pretnje sa druge strane, ne mogu na pravi način uspostaviti arhitekturu bezbednosti. Štaviše, danas su planovi kontinuiteta poslovanja i upravljanje rizikom osnovni elementi u definisanju i poslovne arhitekture organizacije, i izostavljanje ovog koraka u upravljanju košta mnogo u narednim fazama, i negativno utiče na mogućnost donošenja ispravnih odluka i kontrolu troškova.

U ovom koraku treba nabrojati procenjene rizike, pretnje za informacionu imovinu i identifikovati kritične poslovne procese koji zbog uočenog rizika uslovljavaju potrebu za zaštitom (poslovanje na Internetu, reputacija brenda, prevencija krađe, prevencija gubitka, ispunjavanje standarda i zakonskih obaveza, usaglašenost sa propisima, realizacija kontinuiteta poslovanja).

U IT sektoru centralne banke je prihvaćena metodologija Evropske centralne banke (ECB), te se upravlja i informatičkim (IRM) i operativnim (ORM) rizikom. U sklopu upravljanja IRM radi se procena kritičnosti (CA) za svaku aplikaciju odmah nakon zahteva za izradu, i kasnije kod većih promena ili periodično. Procenjuju se stepeni kritičnosti (rizik) s obzirom na moguće narušavanje poverljivosti, integriteta i dostupnosti, i s obzirom na to ispostavljaju bezbednosni zahtevi. Na osnovu bezbednosnih zahteva određuju se mere i kontrole, te se zajedno sa poslovnom stranom (naručiocem) odlučuje koje će se od njih prihvatiti i implementirati, a gde će se prihvatiti rizik.

I zahtevi i mere i kontrole nalaze se u *Katalogu kontrola* bezbednosti, napravljenom na osnovu ISO 27002. CA se radi samo za aplikativne projekte, ne i za infrastrukturne.

Operativni rizik dat je u dokumentu koji navodi procenjene operativne rizike, daje procenu njihovog uticaja i predloge za smanjenje. Periodično se revidira. Uspostavljeno je takođe i upravljanje incidentima i to kroz SD, kao i redovno izveštavanje.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 1.2.**

3.3. Kontekstualna bezbednost – Proces

Poslovni model procesa odgovor je na pitanje: Kako? Budući da su upravo poslovni procesi konkretizacija prelaska puta od ciljeva do realizacije, jasno je da se upravo tu dešava (obrada informacija i transakcije) i nalazi (imovina) sve ono što treba zaštititi. Zadatak organizacije je da mapu procesa izradi u ranoj fazi postavljanja poslovne arhitekture. Mapa procesa se ne koristi isključivo za bezbednosnu arhitekturu, ona je jedan od ključnih elemenata dokumentovanja rada svake organizacije. Mapa procesa koja se koristi namenski za definisanje parametara informacione bezbednosti, može se predstaviti kao redukcija mape procesa organizacije na samo one procese koji uključuju IKT podršku i samim tim zahtevaju mere IKT bezbednosti, a predmet su upravljanja rizikom i ključni za dostizanje ciljeva organizacije.

Dobar okvir za izradu mape procesa je okvir COBIT standarda, zato što omogućuje menadžmentu da premosti jaz između zahteva kontrole, operativnih rizika i poslovnih rizika, a takođe pruža i jasnu sliku IKT kontrola nad procesima i povezuje poslovne ciljeve sa IKT ciljevima.

Nadalje, mapa procesa na svojim nižim nivoima pruža kompletnu sliku poslovnih interakcija i transakcija, kao i šemu poslovne komunikacije.

IKT centralne banke ima izrađenu mapu procesa prema COBIT5 okviru, pri čemu su procesi podeljeni na

1. Procese organizacije, planiranja i usaglašavanja
2. Procese izgradnje i implementacije
3. Procese isporuke, servisiranja i održavanja
4. Procese monitoringa, evaluacije i procene

Svaki segment ima tri sloja L0 – osnovni, globalni nivo, L1 – procesi i L2 – podprocesi i/ili niže aktivnosti.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 1.3.**

3.4. Kontekstualna bezbednost – Ljudi

Pitanje „ko“ u prvom sloju bezbednosne arhitekture postavlja se da bi se definisao organizacioni okvir u kome se implementiraju bezbednosne mere. To obuhvata ne samo krajnje izvršioca posla odnosno korisnike IKT, već prvenstveno upravljačke i rukovodeće strukture, lance dobavljača, outsorsing partnere, strateške partnere, a na kraju i sve ostale partnere koji utiču na poslovne funkcije organizacije. Konkretno, bitno je definisati vrste odnosa koji postoje između organizacije i svake od ovih kategorija, posebno kad se radi o eksternim partnerima.

Potrebno je navesti dokumentaciju i regulativu koja uređuje ove odnose, tu su prvenstveno pravilnici koji regulišu oblast rada, prava i obaveza, kao i etičke norme u obavljanju posla. Kad su u pitanju korisnici IKT odnosno izvršioci posla, važan podatak su njihovi nivoi ovlašćenja, odnosno postojanje minimalnog skupa ovlašćenja koji je dovoljan da se nesmetano odvijaju radne operacije. Važno je jasno i nedvosmisleno odrediti nivo posvećenosti upravljačkih i rukovodećih struktura bezbednosti, čak i ako je ona mala, jer je to onda signal da se identifikuje rizik i da se ta oblast preispita u nekom od narednih PDCA⁴ ciklusa. Kad su u pitanju eksterni partneri, dobavljači, outsorseri i drugi partneri, potrebno je utvrditi postojanje ugovora, kao i dodatnih akata kao što su memorandum, i veoma važne izjave o neodavanju poslovnih tajni.

Druga dimenzija ljudskog faktora u konceptualnoj bezbednosti je definisanje relacije između ljudi i samih bezbednosnih mehanizama, čije korišćenje mora biti lako, bezbedno i ne sme narušavati poslovni proces kao ni motivaciju i samopouzdanje zaposlenih.

U centralnoj banci evidencija zaposlenih je vezana sa Identity Manager (IM) rešenjem, pri čemu se u IM dodeljuju i prava na određene IKT resurse. IM prati sve promene u statusu zaposlenog, tako da se promene nivoa ovlašćenja dešavaju automatski. IM je takođe vezan na Active Directory (AD). Politika upravljanja bezbednošću propisuje da se svakom korisniku dodeli minimalan skup ovlašćenja potreban za obavljanje dodeljenog posla.

Ugovori sa eksternim partnerima se vrlo pažljivo i detaljno analiziraju pre potpisivanja, u saradnji sa pravnicima, a implementirana je i obaveza potpisivanja dokumentata kojima se reguliše neodavanje (NonDisclosure Agreement – NDA)

IT sektor centralne banke je u procesu izrade i implementacije SLA (Service Level Agreement) između poslovnih funkcija banke i IKT sektora, da bi se na osnovu toga pristupilo i izradi SLA sa eksternim dobavljačima. Problem je što je telekomunikaciona infrastruktura u vlasništvu jednog preduzeća koje zbog monopolskog položaja nema interesa da potpisuje SLA, a budući da je to centralna usluga, ograničava i ostale potencijalne SLA.

⁴Plan-Do-Check-Act, Demingov ciklus, primjenjivo na SABSA model, ISO 27k, i preporučen pristup u implementaciji ISMS

Zaposleni su sa bezbednosnim mehanizmima upoznati kroz programe podizanja svesti, a prate se i povratne informacije (povremena testiranja), da se vidi da li su svi mehanizmi shvaćeni i prihvaćeni od strane korisnika i dovoljno jednostavni za korišćenje da ne ometaju proces rada.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 1.4.**

3.5. Kontekstualna bezbednost – Lokacija

Poslovna geografija predstavlja skup informacija o lokacijama na kojima se odvijaju poslovni procesi, o lokacijama komponenti IKS, te o bezbednosnim aspektima datog rasporeda. Tu su takođe i specifični uslovi poslovanja na određenim lokacijama (ekonomski, vremenski, pravni, kulturološki, klimatski) i eventualne razlike, te rizici koje te razlike proizvode. Za informacionu bezbednost vrlo je važno da se lokacijski dobro definišu svi poslovni sistemi koji su distribuirani, na bilo koji način. Čak i ako se organizacija nalazi samo u jednoj zgradi, ona takođe može biti u velikom stepenu lokacijski složena i distribuirana. Može imati različite načine udaljenog pristupa (Internet, VPN, ... udaljenu lokaciju DR sajta⁵..), a ako posluje kao internacionalna važno je voditi evidenciju o svim razlikama u zakonskim okvirima i prihvaćenim standardima. Ukoliko se bezbednosna arhitektura implementira nakon što je poslovna i IKT arhitektura već postavljena, a što je često slučaj, ovaj korak je važan u dobijanju odgovora kako se predloženo bezbednosno rešenje uklapa u već postojeću infrastrukturu.

Posebno kad se ima na umu primena bezbednosnih rešenja, moguće je da nećemo moći primeniti isto rešenje na različite lokacije, i zato je važno da se ova analiza uradi detaljno i korektno, čime se u ranoj fazi izbegavaju greške i dodatni troškovi implementacije bezbednosnih rešenja.

Poslovna geografija centralne banke obuhvata šest lokacija u Beogradu, i po jednu u Novom Sadu, Užicu, Nišu i Kragujevcu. Mrežna infrastruktura je dobro postavljena, uređaji su unificirani, te je i zaštita na mreži ujednačena i dovoljno redundantna da ne ostavlja prazne prostore. Upravljanje konfiguracijom, antivirus, antimalver – radi se centralizovano pomoću agenata na radnim stanicama, tako da ne zavisi o geografskoj lokaciji. Na isti način rešeno je i upravljanje mrežom. Pojedine kritične poslovne funkcije imaju DR lokacije kojima se takođe može upravljati kroz mrežu, ali istovremeno imaju redundantni pristup i napajanje.

Distribucija aplikacija rešena je na nekoliko načina: klasične web aplikacije sa pretraživačem u funkciji klijenta, Oracle Forms aplikacije sa web filozofijom (plugin na klijentu), ClickOnce distribucija, klasična klijent-server distribucija.

Procesom virtualizacije obuhvaćeno je 95% resursa (bez radnih stanica), što umanjuje značaj fizičke lokacije, ali povećava potrebu za obezbeđenjem virtualnog okruženja.

⁵DR – Disaster Recovery, paralelna instalacija istog ili osnovnog IKS za obezbeđenje kontinuiteta poslovanja. Standardi predviđaju minimalnu udaljenost od 50 km, a postoje i drugi kriterijumi, npr. Niš je na većoj udaljenosti od Beograda, ali je Novi Sad na različitoj tektonskoj ploči.

Centralna banka nema lokacije u drugim državama (ovo se očekuje tek pri ulasku u EU), tako da nisu analizirani inostrani propisi i standardi. Kao i u ostalim aspektima razvoja, primenjuju se principi najbolje prakse i preporuke ECB. Takođe, centralna banka ne drži svoje podatke u oblaku, niti za sada ima implementiranih *cloud-based* rešenja.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 1.5.**

3.6. Kontekstualna bezbednost – Vreme

U kontekstualnom sloju bezbednosne arhitekture, vremenska odrednica odnosno odgovor na pitanje *kad*, zapravo su vremenske zavisnosti poslovnih funkcija. To su zapravo oni aspekti bezbednosti koji se odnose na poslovne funkcije i njihovo odvijanje u vremenu, vezane za tačne satnice ili periode, vezani za vremenske zone. Tu su i funkcije ograničene brzinom izvršavanja, količinom informacija u vremenu, životnim ciklusima pojedinih procesa, zatim postojanje procesa koji se dešavaju u realnom ili tačno određenom vremenu, procesa koji su vremenski uslovljeni tržištem ili zahtjevaju brzu reakciju na neki događaj spolja.

Svi ovi faktori, odnosno vremenske specifičnosti pojedinih poslovnih funkcija važan su parametar za bezbednosne mehanizme, jer njihova aktivnost mora biti usklađena u vremenu sa odvijanjem poslovnog procesa. Radi se zapravo o definisanju raspoloživosti mehanizma zaštite i to u terminima kako performansi tako i perioda. Neusklađenost vremena primene bezbednosnih mehanizama i obavljanja poslovnih funkcija rezultuje povećanim rizikom i troškovima, kao zbog potencijalnog gubitka usled nepravilno uspostavljenih mera, tako i zbog nerentabilno instalirane zaštite. Prilikom dokumentovanja ovog dela konceptualnog sloja važno je uočiti i predviđanja za buduće funkcije, ili one koje su u razvoju (na primer 24/7 web servis), da bi se mehanizmi zaštite na vreme planirali.

IKT centralne banke analizira poslovne zahteve sa stanovišta vremenske odrednice kroz zahteve za raspoloživošću, i prema tome se upravlja i pri primeni mera bezbednosti. Jedna od mera je na primer i centralizovano gašenje radnih stanica koje korisnici ostave uključene, nakon isteka radnog vremena. Izuzetak su IDS/IPS sistemi, kao i ostali elementi mrežne zaštite koji rade neprestano, bez obzira na radno vreme, budući da WEB servisi rade 24/7. Nadalje, u neradno vreme povećani su pristupi putem VPN linka, tako da taj servis mora uvek biti raspoloživ.

Svi objekti centralne banke su u istoj vremenskoj zoni, a vreme na mreži je centralno upravljano sa servera namenjenog za to.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 1.6.**

4. Konceptualna bezbednost

Nakon definisanja konteksta bezbednosne arhitekture, sledeći sloj, konceptualna arhitektura, predstavlja pogled arhitekta sistema zaštite. Ovaj sloj najbolje se može shvatiti ako se pretpostavi da je arhitekta kreativna osoba sa vizijom [1] kome je izazov da razume poslovne zahteve i rizike koje nosi i na osnovu toga napravi pravi izbor logičkih i fizičkih komponenti budućeg bezbednosnog rešenja. I ovde se vidi potreba za poslovnim analitičarem, upravo zbog prethodno pomenutog rizika da arhitekta bezbednosti u želji da primeni savremena bezbednosna rešenja izgubi iz vida potrebu posla. Zato se pažljivo bira tim koji će pokriti kako oblast zaštite na višem nivou, tako i oblast potpunog razumevanja zahteva poslovnih procesa. Ovaj pogled, dakle, treba da sadrži viziju bezbednosnog rešenja u osnovnim crtama, koja će biti priprema za naredne korake u kojima će ljudi sa različitim znanjima i veštinama realizovati pojedinačne implementacije.

Jedna od čestih grešaka je da se stručnjaci za pojedina tehnološka rešenja uključe prerano, što može ometati proces svođenjem koncepta na niži nivo apstrakcije i sugerisanjem konkretnih rešenja u fazi kad nema dovoljno preduslova za pravu odluku. Kao što samo ime sugerise, pravi se koncept zaštite koji ispunjava sva očekivanja poslovne strane, a da ih pri tom ne ometa i ne utiče na performanse. Ovde se definišu opšti principi i osnovni koncepti buduće arhitekture, što je vrlo značajno jer su to upravo smernice za kasnije korake koji će se odvijati na nižim nivoima. Takođe, ovde definisani koncepti i principi ostaju nepromenjeni do kraja, u svim narednim slojevima.

4.1. Konceptualna bezbednost – Imovina

Dok je pitanje „šta“ u definisanju konteksta bezbednosti definisalo poslovno okruženje, u konceptualnoj bezbednosti to su **poslovni atributi**. Budući da smo u prvom koraku definisali šta štitimo izrazimo kroz ciljeve organizacije i poslovni kontekst, konceptualni pogled treba da odgovori na to koji su to atributi (što daje poseban pogled na informacije koje se štite), da bi se kasnije definisale logičke i fizičke komponente potrebne za razvoj bezbednosnog rešenja. Ovde je ključno da postoji strategija analize rizika poslovanja. Za razliku od procene rizika korištene za definiciju motivacije konteksta, ovdje se radi o analizi poslovnog rizika koja kao rezultat treba da da one attribute poslovanja koji će biti predmet zaštite. Korisno je da se primeni svojevrsni „inženjering zahteva“ i da se prikupljeni podaci o poslovnim zahtevima na neki način normalizuju i standardizuju.

SABSA okvir se posebno osvrće na profilisanje poslovnih atributa, štaviše, smatra se da je to sama srž SABSA metodologije. Inženjering zahteva je tehnika koja SABSA metodologiju čini jedinstvenom i obezbeđuje vezu između poslovnih zahteva i tehnološkog dizajna i dizajna procesa.

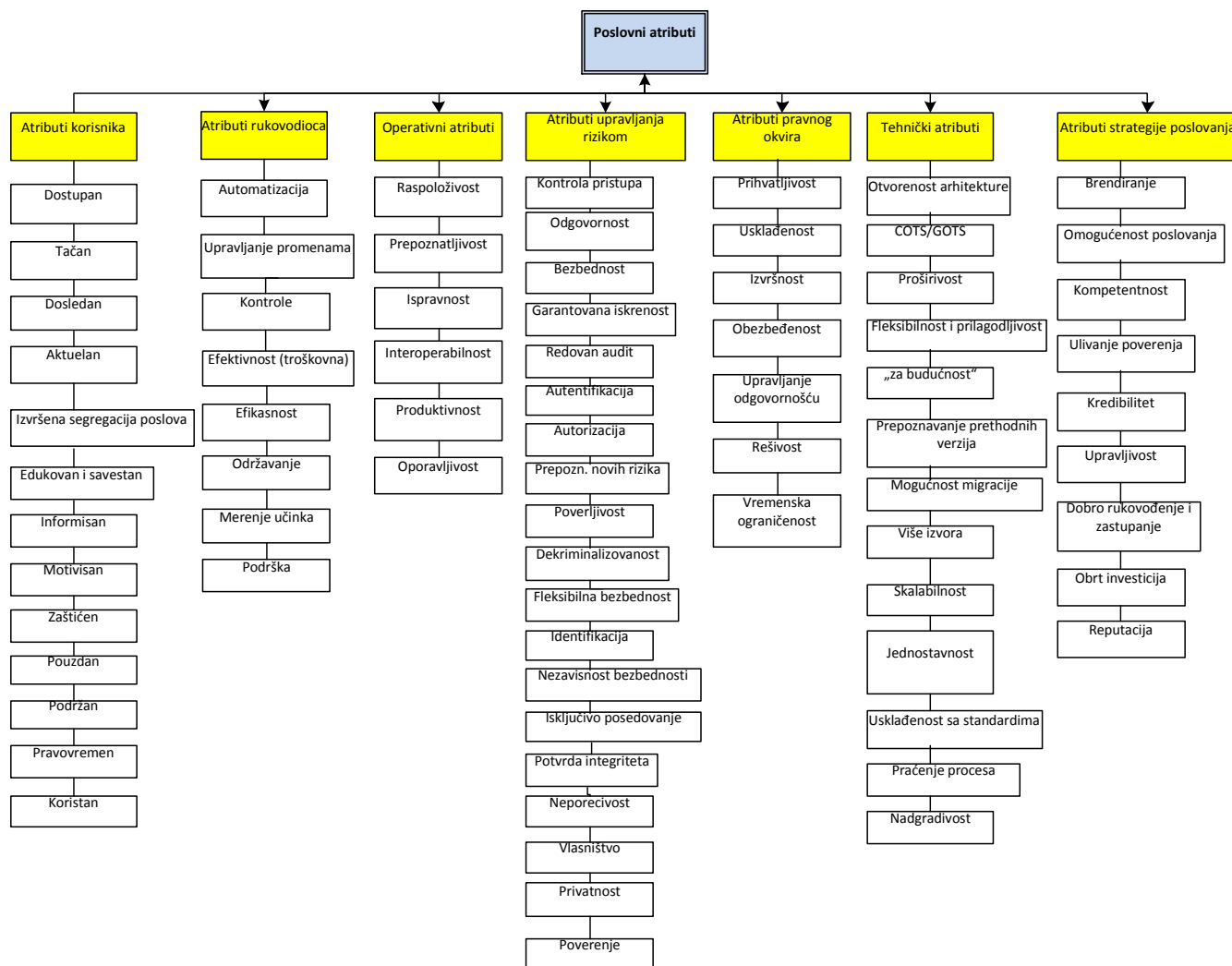
Originalna taksonomija atributa data po SABSA metodologiji data je na Slici 3, i to fokusirana upravo na IKT sisteme i njihova okruženja. Podela je na sedam grupa, pri čemu je svaki poslovni atribut apstrakcija realnog poslovnog zahteva. Prikazana podela rezultat je praktičnih rezultata

dobijenih nakon rada na mnogim organizacijama, tako da daje najširu sliku, i realno je izvući podskup koji će najbolje oslikati pojedinačne potrebe, ali je preporuka da se uzme što više od ponuđenih atributa. Nadalje, za svaki od njih treba razviti vlastitu metriku, SABSA preporuka je poseban pristup za svaki atribut[2].

Nakon ovoga radi se tzv „profilisanje atributa“, pri čemu profil obuhvata one attribute koji su relevantni za specifičan posao organizacije. Ukoliko nedostaju, mogu se dodati atributi i van predloženih. Profil je jedan ili više zavisno od složenosti organizacije i nivoa detaljnosti procene rizika. Primer profila dat je u **Prilogu 3**, iako bi možda neka poslovna funkcija bila bolji primer, pokazan je zapravo princip profilisanja.

Za početak, u IT sektoru centralne banke korišćena je predložena taksonomija, s tim što se od ponuđenih atributa izabrao podskup značajnijih, da se u prvoj fazi uzmu u obzir. Ovo će se realizovati kroz obavezne i opcione attribute. Od atributa datih na **Slici 3**, centralna banka kreće sa jednom polovinom onih koji su obavezni, ostali su opcioni. Za sada nije prepoznat nijedan dodatni atribut, iako je verovatno da će se to desiti u narednim fazama, zbog specifičnosti institucije.

Takođe, realno je da se u narednim fazama uradi profilisanje, te da se za posebne poslove odredi i skup relevantnih atributa. Nakon što se savlada profilisanje na primeru IT sektora (grupa *Administratori operativnih sistema*, na primer, može imati poseban profil), razvija se dobar alat za primenu profilisanja i na poslovne funkcije cele banke, kad dođe do rada na krovnoj arhitekturi.



Slika 3. Taksonomija poslovnih atributa po SABSA [1]

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 2.1.**

4.2. Konceptualna bezbednost –Motivacija

Odgovor na pitanje: *zašto* je važna zaštita odabranih informacija? - je zapravo opis ciljeva koje želimo postići kontrolama. Jasnim navođenjem ciljeva objašnjava se i *zašto* je zaštita važna, odnosno može se sagledati šta bi za organizaciju značilo da se ciljevi ne postignu. Ponekad je u razgovoru sa najvišim rukovodstvom dobro koristiti strategiju prikazivanja hipotetičkog stanja u slučaju da se ne primene bezbednosne mere. Budući da je ROI teško iskazati kad je u pitanju bezbednost, ovakva, „inverzna“ argumentacija daje intuitivno jasnu sliku motiva i interes organizacije.

Kontrole koje se primenjuju nastaju upravo iz analize operativnih rizika procenjenih nad poslovnim atributima, i to po svakom profilu ponaosob (ovde je jasno vidljivo zašto „matrica“, jer se vidi uticaj sadržaja 1.2. kao i 2.1.). Dakle, profil je sad ono sa čime se nadalje radi. Rezultat analize rizika za profil su oni atributi koji će biti obuhvaćeni zaštitom, da bi se postigao zadati cilj. Tu je vidljiva upravo konceptualizacija poslovne motivacije da se uvede bezbednost.

Poverljivost, integritet i raspoloživost su ciljevi zbog kojih se uspostavljaju bezbednosne kontrole u IT centralne banke. Budući da IT sektor postoji kao podrška ukupnom poslovanju, a da je poslovanje centralne banke isključivo oslonjeno na IKT, svi rizici se zapravo preslikavaju, i kritičnost aplikacija procenjena u IT sektoru je zapravo ujedno i kritičnost funkcije koju aplikacija pokriva, te se u izboru mera i kontrola za pojedino IKT rešenje zapravo biraju i kontrole za dati poslovni proces, a sve u cilju prevencije narušavanja poverljivosti, integriteta i raspoloživosti.

Neka od narednih faza razvoja bezbednosne arhitekture u centralnoj banci obuhvata profilisanje, pa samim tim i specifične rizike po profilima, što nije predmet ove analize.

Konceptualni pogled rizike definiše kao verovatnoće nepostizanja ciljeva, i smisao kontrola je da se te verovatnoće smanje. U slučaju centralne banke, postojanje reputacionog rizika, i transfer rizika na čitav finansijski sektor uslovljava da su zahtevane verovatnoće, odnosno prihvatljivi rizici, vrlo mali.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 2.2.**

4.3. Konceptualna bezbednost – Proces

Kako dostići željeni nivo zaštite poslovnih procesa, sa raspoloživim tehnologijama i u datim organizacionim uslovima? Sa jedne strane imamo strategiju zaštite iskazanu između ostalog i kroz politike, a sa druge procesni okvir koji opisuje sve poslovne promene. Koncept je ovde upravo primena bezbednosne strategije uz uvažavanje slojevitosti arhitekture, tako da zaštita bude prisutna na svim slojevima u potrebnom stepenu. Bitno je prvenstveno prepoznati individualne taktičke elemente zaštite na nižim stepenima, i integrisati ih u ukupnu zaštitu tako da se uklapaju ne menjajući smisao zaštite i strateške ciljeve. (Na primer: nepotrebno je da fizičko obezbeđenje zadržava opremu posetilaca, jer na višem nivou postoje mehanizmi koji ne dozvoljavaju da se oprema trećeg lica priključi na mrežu).

Generalno, strategije po slojevima uključuju: aplikativnu bezbednost, bezbednost mreže, PKI strategija, kontrola pristupa preko rola (RBAC) i slično.

Takođe, za svaku grupu poslovnih zahteva (potrebno je izvršiti ukupnjavanje gde god je moguće, pa tako i poslovne zahteve prema vrsti resursa i sličnoj arhitekturi) koja je prepoznata

kroz bezbednosnu arhitekturu (npr, web servisi, mejl, IP telefonija, SAP, ...) treba da postoji bezbednosna strategija (ili više njih) koja tu poslovnu kategoriju podržava.

U centralnoj banci primenjena je slojevita zaštita, odnosno „zaštita u dubinu“, a pored toga, iz perspektive poslovnih zahteva i različitih servisa prepoznate su sledeće bezbednosne strategije:

1. Mrežna zaštita (Firewall, IDS/IPS, web filtriranje, ...)
2. Antivirus i antimalver zaštita
3. Bezbednosni standardi operativnih sistema
4. Bezbednosni standardi razvojnih okruženja
5. Bezbednosni standardi specifičnih rešenja (IP telefonija, virtuelna infrastruktura, EBS, exchange serveri, aplikativno rešenje za upravljanje dokumentima, protokoli za razmenu podataka, platni sistem, centar za platne kartice, specijalne službe u kovnici novca, itd.)
6. Aplikativna bezbednost
7. Fizičke kontrole
8. PKI i enkripcija
9. Korelacija logova - SIEM
10. Programi za podizanje svesnosti
11. Upravljanje rizikom
12. Kontrola kvaliteta

Spisak nije konačan, predstavlja pogled na procesnu komponentu konceptualnog sloja i daje okvir i smernice za razumevanje.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 2.3.**

4.4. Konceptualna bezbednost – Ljudi

Koncept personalnog rešenja zahteva da se definiše ko će biti uključen u upravljanje bezbednošću za vreme korišćenja IKT rešenja u produkciji. Na ovom nivou radi se podela uloga i odgovornosti (od upravljačkih funkcija do krajnjih korisnika) , kao i načini komunikacije i stepen poslovnog poverenja između strana (npr, da li se radi o interno održavanom IKT rešenju ili postoji usluga trećeg lica, da li postoji SLA ili ne, i sl.). Navodi se takođe i ko je vlasnik imovine i podataka, ko su zastupnici i krajnji korisnici, te treća lica koja isporučuju određene servise.

Pomenuti koncept poverenja, (dokumentovan ugovorima, dogovorima, memorandumima, sporazumima, preuzetim obavezama, ali i politikama) je važan jer reguliše odnose kako entiteta unutar organizacije tako i organizacije sa spoljnim saradnicima. Na ovom nivou koncept obuhvata konkretnu rolu koju obavlja pojedinac i/ili grupa, jer je bitno stvoriti osnovu za utvrđivanje odgovornosti, što nije moguće sa bezličnim konceptima kao što su „poslovni proces“, „poslovna funkcija“ i slično.

U primeru IT sektora centralne banke ovaj koncept je jako važan, budući da se radi o relativno velikom broju ljudi koji su pritom razmešteni po različitim lokacijama. Upravljačka funkcija definisana je kroz odgovornost koja je, zbog specifične organizacije, podređena direktno najvišem rukovodstvu centralne banke, što zahteva dodatnu pažnju, analitičnost, ali i znanja i veštine kako u struci tako i u rukovođenju. Kad su u pitanju bezbednosna rešenja, kao što je već pomenuto u odeljku 1.1., poseban izazov rukovodstvu IKT je kako najvišem rukovodstvu organizacije predstaviti potrebu za ulaganjem u nešto što nema očigledan ROI. U tu svrhu, a i radi povećanja kredibiliteta odluka, formirano je upravljačko telo Odbor za bezbednost, koje je sastavljeno od rukovodilaca IKT u proširenom sastavu, pojedinih rukovodilaca poslovnih celina i najvišeg rukovodstva centralne banke.

Kad su u pitanju zaposleni u IT sektoru, njihove odgovornosti, prava i obaveze su definisane kroz ograničenja preslikana u IM i AD, kao i za sve ostale zaposlene, samo što zbog potrebe posla ta ovlašćenja imaju veći stepen nego za krajnje korisnike IKT rešenja. Iz tog razloga je i odgovornost veća. Prava nad pojedinim resursima moraju biti predmet redovnih revizija.

Odnos sa trećim licima i nivoi poverenja definisani su potpisanim ugovorima i sporazumima, a postoji i kategorizacija partnera prema poverenju. Nadalje, tu su procedure koje regulišu boravak trećih lica u prostorijama banke, odgovornosti i obaveze.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 2.4.**

4.5. Konceptualna bezbednost – Lokacija

Lokacija primene zaštite deluje kao jednostavan zadatak, međutim, treba imati na umu da se ne radi o samoj lokaciji implementacije, već o potrebnoj pokrivenosti i načinima kontrole da je taman onolika pokrivenost koja je potrebna i implementirana, te da nema segmenata koji nisu obuhvaćeni .

Ključni pojam ovde su upravo bezbednosni domeni, koji mogu biti logički i fizički. Određivanje granica bezbednosnih domena najčešće se poklapa sa već postojećom arhitekturom (ActiveDirectory, zgrade, LAN mreža, SMTP ..) , ali isto tako mogu biti i dodatno izgrađeni za specifične poslove (WEB portal, prenos podataka, specifične, viskokorizične funkcije kao platni sistem i slično).

Kod vezivanja za postojeće domene bitno je voditi računa o implikacijama koje promene u konfiguraciji tih domena imaju na bezbednost.

IKT centralne banke kontroliše domene na nekoliko načina, tu su mrežni domeni odvojeni LAN mrežama i granama unutar mreža, zatim domeni u AD, načini na koje korespondiraju domeni između AD, SD, IM. Postoji potpuno preslikavanje ovih domena na polje bezbednosti, jer svi bezbednosni uređaji i strategije prate organizaciju ovih domena. Za specifične slučajeve i

povremene poslove mogu se kreirati i specifični bezbednosni domeni: npr. grupa studenata na praksi ili pripravnika, učesnici konferencije za koje se privremeno obezbeđuje pristup i izoluje pristupna tačka za bežični pristup internetu, i slično.

Kada se radi o distribuciji aplikacija, zatvorena okruženja poput Oracle razvojnog okruženja, ili .NET okruženja imaju svoje standarde, što olakšava definisanje bezbednosnog domena i poverenje u distribuciju. Web aplikacije postavljaju poseban izazov ako korisnici pristupaju sa Interneta, što ima razloge i u pravnoj neregulisanosti ove oblasti u našoj zemlji.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 2.5**.

4.6. Konceptualna bezbednost – Vreme

Posmatranje kroz koncept životnog ciklusa je najčešće korišćena metoda u implementaciji kako servisa, tako i procesa, tako da se može pronaći i u ITIL-u i COBIT-u, te u mnogim standardima i metodologijama za praćenje projekta. Jedna je i od ključnih postavki u upravljanju rizikom.

Životni ciklusi i rokovi omogućuju da se određeno IKT rešenje prati kroz produkciju upravo onoliko koliko zaista produktivno radi, te da se nakon toga izvrši njegovo penzionisanje i uklanjanje svih bezbednosnih mehanizama koji su bili implementirani. Ovde zapravo govorimo o relevantnim nivoima zaštite kroz vremenske cikluse.

Upravljanje rizikom takođe može kao izlaz dati zahtev za povećanjem nivoa zaštite za određeno rešenje u određenom periodu njegovog životnog ciklusa (ukoliko imamo npr. stariju opremu ili nove pretnje za određeni tip infrastrukture).

Upravljanje životnim ciklusom IKT u IT sektoru centralne banke prati se kroz upravljanje projektom, upravljanje promenama i servisnim pristupom u celini. Usvojene su preporuke ITIL-a, i na taj način su uređeni procesi i dokumentacija. S tim u vezi, bezbednosna rešenja su uklopljena u sve faze životnog ciklusa, što obezbeđuje adekvatnu pokrivenost i usklađenost.

Prvi korak je da se prilikom implementacije novog rešenja i/ili servisa, kao i prilikom početka razvoja nove aplikacije proceni inicijalni rizik, te utvrde bezbednosni zahtevi i kontrole. Upravljanje rizikom podrazumeva regularno periodično obavljanje revizije rizika i pretnji, što obezbeđuje da zaštita bude aktuelna i adekvatna u meri u kojoj se rukovodstvo odluči za umanjenje rizika na ovaj način. Za sva rešenja i servise implementirane pre uspostavljanja procedura koje definišu procenu kritičnosti i određivanje bezbednosnih zahteva i mera, ove se procene rade retroaktivno.

Servisi koji više nisu u upotrebi, a nisu se na odgovarajući način povukli i „penzionisali“ mogu predstavljati ne samo balast već i opasnost za ostatak sistema, te je potrebno raditi redovne revizije servisa kojima se dugo nije pristupalo, i analizirati uslove njihovog povlačenja.

Takođe, bitno je pratiti preporuke proizvođača opreme i softvera kojima se definišu rokovi upotrebe, termini prestanka podrške, izlazak novih verzija, zakrpa i slično, kao i ugovore za održavanje da se prate garantni rokovi i vremenske odrednice za održavanje.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 2.6.**

5. Logička bezbednost

Logički sloj razvoja bezbednosne arhitekture zove se još i **pogled dizajnera** zaštite. U materijalnom svetu bi se to moglo uporediti sa poslom gde dizajner preuzima koncept od arhitekta i njegov zadatak je da interpretira arhitektin konceptualni pogled i od njega kreira logičku strukturu koja može poslužiti da se na osnovu nje izgradi konkretan objekat. Dok je arhitekta umetnik i vizionar, dizajner mora biti inženjer. To je posao koji se u IKT svetu zove sistem inženjering. U okviru tog procesa potrebno je prepoznati i popisati sve logičke objekte arhitekture celog sistema. Konkretno, ovde u igru ulazi pregled konkretne IKT imovine, konkretne politike upravljanja rizicima, postupci i procedure za korišćenje IKT servisa, strane u ugovorima i sporazumima, modeli poverenja, lokacije sa vezama i tokovima podataka između njih, tačan sled događaja.

Ovaj sloj modelira poslovni proces kao sistem, sa svim njegovim komponentama koje mogu biti elementi ili podsistemi. Glavni elementi bezbednosti koji su koncipirani kroz arhitekturu sad se pojavljuju kao konkretni (doduše još na logičkom nivou); bezbednosni servisi i opisuju logički tok kontrola i veze među tim logičkim elementima. Negde se može čuti i izraz „logička arhitektura bezbednosti“, i ovo postaje sve važnije u savremenim organizacijama, pogotovo onim velikim sa raznorodnom arhitekturom, velikom mrežom i velikim brojem različitih platformi i uređaja. Bez dobro postavljene logičke arhitekture bezbednosti može se desiti da se rešenja implementiraju parcijalno, što za posledicu ima povećanje troškova, povećanje posla, neadekvatnu zaštitu, redundantne kontrole, a na kraju može rezultovati ili demontiranjem rešenja, ili njegovim zaobilaženjem.

Nadalje, logička arhitektura postavljena na ovom sloju mora verno da predstavlja koncepte predstavljene u prethodnom koraku, ona je i svojevrsna verifikacija koncepta: ukoliko na konceptualnom nivou nešto nije dobro sagledano, ovde može da se uoči i ispravi greška. Na ovom nivou se sve sa viših nivoa predstavlja u obliku logičke apstrakcije i priprema za fizičku izvedbu.

5.1. Logička bezbednost – Imovina

Ono što na logičkom nivou predstavlja poslovne procese, odnosno poslovanje, i što treba da se štiti su zapravo poslovne informacije. Preko poslovnog okruženja tj. konteksta, i koncepta odnosno poslovnih atributa, na ovom sloju se dolazi do sledećeg nivoa apstrakcije, a to je poslovni informacioni model.

Ovde se identifikuju poslovne informacije kao logička interpretacija stvarnog poslovanja. One su predmet zaštite, budući da je potrebno obezbediti njihovu razmenu i čuvanje, ali isto tako i dostupnost strukturama odlučivanja. Na ovom nivou već govorimo o informacijama, te se može identifikovati osnovna motivacija za zaštitom, a to je obezbeđenje poverljivosti, integriteta i dostupnosti poslovnih informacija.

IT sektor centralne banke ima dobro razrađenu identifikaciju poslovnih informacija, budući da se veći deo informacionog sistema razvija u kući, a i onaj koji nije ima zadužene sistem analitičare koji prate i podržavaju korisnike (EBS, EDMS, IP telefonija ...). Za nekoliko poslovnih funkcija koje imaju IKT funkcije koje nisu u potpunosti integrisane u IKT (platni sistem, kartice) planirana je i razrađena potpuna integracija, što će omogućiti da se poslovne informacije centralne banke u potpunosti mogu sagledati kroz poslove IT sektora. Ovo je značajno upravo sa aspekta obezbeđenja zaštite.

Informacioni modeli konkretno su opisani kroz šeme baza podataka i projektnu dokumentaciju. Procena kritičnosti (CA), sa druge strane, daje informacijama stepen rizika za narušavanje poverljivosti, integriteta i dostupnosti, te postavlja bezbednosni okvir, kao što je već ranije objašnjeno. U ovoj fazi, sekcija 3.1. u Prilogu 2 sadržavaće kako referencu na šeme baza podataka, tako i konkretne IRM dokumente, po aplikacijama. Za infrastrukturne projekte (npr. virtuelna infrastruktura) tu je projektna dokumentacija i/ili bezbednosni okvir koji garantuje proizvođač.

Kad je reč o čuvanju informacija to je definisano pravilnicima na nivou centralne banke, dok su konkretne izvedbe i načini rukovanja informacijama koje nisu predmet pravilnika definisane procedurama bekapa.

Bezbednost razmene informacija je vrlo važna stavka, i ovde treba nabrojati sve protokole koji se koriste, kao i načine enkripcije (konkretne izvedbe nad podacima će biti razrađene u sledećem sloju). Tako na primer, kod razmene statističkih podataka s bankama koristi se enkripcija, u platnom sistemu PKI, a i jedno i drugo se obavlja preko privatnih linija.

Takođe, potrebno je navesti i konkretne mehanizme kojima se obezbeđuje poverljivost, integritet i dostupnost, što će se takođe razraditi u narednom sloju. Previše mehanizama može ukazivati na nepotrebnu diversifikaciju i potrebu standardizacije rešenja.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 3.1.**

5.2. Logička bezbednost – Motivacija

Zašto poslovne informacije zahtevaju zaštitu? Kao i na dosadašnjim slojevima, motivacija je uvek vezana za rizik. Bezbednost i rizik ne idu jedno bez drugoga, jer implementacija bezbednosnih mera i kontrola ne bi ni postojala bez postojanja rizika. Osnovni okvir za

umanjenje rizika kojima su izloženi IKT sistemi i poslovni procesi podržani sa IKT su bezbednosne politike.

Na ovom nivou definišu se opšte bezbednosne politike i politike upravljanja rizikom, ali isto tako i pojedinačne politike kao što su npr. politike vezane za upravljanje nekim visokorizičnim procesima, politike autorizacije, politike pristupa sistemu, politika sertifikacije i digitalnog potpisivanja, politike lokalnih domena i slično, a sve u cilju obezbeđenja poslovnih informacija.

IT sektor centralne banke predlaže, a na nivou banke se donose Politike upravljanja bezbednošću IS. Ovde su pokrivene sve oblasti koje tretira ISO27002, i može se reći da kao krovni dokument zadovoljava osnovne potrebe. Implementacija arhitekture bezbednosti upravo ovde može da pokaže da postojanje posebnih sub-politika koje definišu pojedine oblasti (kontrola pristupa, pristup Internetu, mobilni uređaji i slično) podiže bezbednost na viši nivo i konkretno se određuje prema određenim problemima bitnim za zaštitu informacija. Budući da se radi o oblasti za koju je uvek postojala svest o važnosti uređivanja, postoje mnogi dokumenti koji pojedinačno definišu određene oblasti bezbednosti, i potrebno je izvršiti njihovo sređivanje, integraciju u politike, i proveriti da ne postoji dokumentacija koja je međusobno neusklađena.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 3.2.**

5.3. Logička bezbednost – Proces

Na logičkom nivou proces zaštite je zapravo logički prikaz kako će poslovne informacije biti zaštićene. Politika bezbednosti u praksi se sprovodi putem bezbednosnih servisa. Ovde se navode **logički bezbednosni servisi** s obzirom na funkciju koju treba da obave (npr. autentifikacija korisnika, zaštita poverljivosti, zaštita integriteta, neoprecivost, garantovana bezbednost sistema, internet filtriranje itd.) i načini kako se oni uklapaju zajedno kao gradivni blokovi jednog kompleksnog bezbednosnog sistema koji treba da pokrije sve poslovne zahteve.

Bezbednosni sistemi zapravo realizuju aktivnosti koje su odgovarajuće pretnjama za bezbednost informacionih sistema. Upoređeni su sa gradivnim blokovima, što s jedne strane ukazuje i na mogućnost selektovanog upravljanja, oni se mogu uključivati selektivno i po potrebi (zbog velike cene i potencijalnog narušavanja performansi), tamo gde i tada kad su potrebni.

Prihvaćena je opšta podela na šest bezbednosnih servisa [5]:

1. Servis poverljivosti
2. Servis integriteta
3. Servis autentifikacije
4. Servis kontrole pristupa
5. Servis neporecivosti
6. Servis onemogućavanja odbijanja usluge (dostupnost usluge)

Za ove bezbednosne servise u funkciji gradivnih blokova vrlo je važno obezbediti višestruku iskoristivost. Logički tok bezbednosnih kontrola mora biti uklopljen i u mape procesa, gde se pominje u terminima i jasno se vidi, kao i u funkcionalnim specifikacijama kao jedna od zahtevanih funkcionalnosti.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 3.3.**

5.4. Logička bezbednost – Ljudi

Personalna šema na logičkom nivou daje odgovor na to koje su funkcije i profili zaposlenih koji su uključeni u zaštitu informacija. Na ovom nivou definišu se uloge, njihove međusobne veze i profili privilegija koje imaju, kroz svojevrsnu šemu koja prikazuje specifikaciju entiteta (korisnici, administratori, kontrolori...), attribute koji su im pridruženi (**Slika 3**), njihove odnose i nivoe poverenja. Okvir za ovo je ujedno i šema privilegija.

Ovaj sloj zahtjeva pažljivu razradu, i to smislu uspostavljanja sistema za održavanje ovih repozitorijuma i lakoće njihovog ažuriranja i praćenja, pogotovo kad je u pitanju promena privilegija. Konkretna izvedba definisaće se na fizičkom sloju, ali principi moraju biti postavljeni u ovom koraku.

Kad govorimo o IT sektoru centralne banke, svi zaposleni su uključeni u zaštitu informacija, u manjoj ili većoj meri. Šema privilegija na kompletnom informacionom sistemu prati se većim delom kroz IM, s tim što se pojedini mrežni podsistemi (CISCO oprema, IP telefonija) upravljaju iz posebnih centara. Pojedine evidencije se vode ručno (kao na primer kontrole VPN pristupa). Na nivou operativnih sistema i aplikacija šeme privilegija su obezbeđene kroz role, i to je standardizovan pristup. Princip je dodatno obezbeđen pravilom da se svim resursima pristupa kroz korisnički nalog iz AD.

Budući da privilegije zavise i o radnom mestu i organizacionom delu, kroz IM je realizovano da se, putem povezivanja sa šifarnicima ljudskih resursa, promena u radnom mestu odmah vidi i kroz degradaciju privilegija, ili potpuno ukidanje. Obrnuto ne važi, dodela prava i eskalacija privilegija mora biti odobrena od rukovodstva.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 3.4.**

5.5. Logička bezbednost – Lokacija

Na logičkom nivou, odgovoriti na pitanje: gde, znači zapravo definisati bezbednosne domene (kao i navesti entitete koje sadrže) i njihove međusobne odnose. Ovde će se navesti i opisati bezbednosni domeni koji treba da postoje kako na logičkom tako i na fizičkom nivou, i sve izvedene grupe i podele nastale na osnovu bezbednosnih kriterijuma prema specifičnim poslovima, ovlašćenjima, lokaciji izvođenja radnih zadataka i slično. Dok je koncept lokacije

samo odgovorio na pitanje koji su to domeni na koje se primenjuje zaštita, logički sloj ih pobliže opisuje, tako da se daje odgovor na pitanje gde će bezbednosne mere biti primenjene, a takođe stvara osnov za buduću postavku konkretnih platformi i mreže na sledećem nivou.

Bezbednosni domeni su mehanizmi koji su zamenili liste kontrole pristupa ACL, koje su postale preglomazne i teške, i promovisali Role Based Access Control (RBAC), kontrole prava bazirane na rolama. Domen se sastoji od uređenih parova (objekat, prava pristupa) koji specificiraju za svaki objekat koje su dozvoljene operacije. Zahtevi za izvršavanje neke operacije se uvek izdaju u domenu:

- Subjekat zatraži izvršavanje određene metode nekog objekta
- Moguća je provera da li je operacija dozvoljena u domenu

Opšte poznat primer domena su grupe korisnika, na primer: administratori u grupi “*admin1*” – imaju pristup objektima i koji se odnose na administriranje sistema 1, Oracle inženjeri u grupi “*orazar*” – imaju pristup razvojnom okruženju Oracla, i slično.

Ako se napravi veliki broj grupa i podgrupa, onda je moguće napraviti finu granulaciju prava pristupa. Do problema dolazi kod distribuiranih baza grupa korisnika – sporo je nalaženje subjekata. Rešenje gornjeg problema može biti davanje sertifikata svakom subjektu. Sertifikat sadrži spisak svih grupa kojima subjekat pripada. Sertifikati moraju biti zaštićeni, na primer digitalnim potpisom. Domeni se ukratko posmatraju kao uloge (role): Korisnik se uvek prijavljuje sa ulogom u sistemu, a ona se povezuje sa privilegijama.

IT centralne banke primenjuje RBAC logiku gde god tehnologija to dozvoljava, a to je danas u najvećem broju slučajeva. Takav pristup olakšava administriranje, a takođe obezbeđuje i jednostavnu i dokumentovanu implementaciju bezbednosti.

Izuzetak od implementiranih mehanizama ovlašćenja su pojedine bezbednosne funkcije koje po prirodi ne treba da budu vidljive. Ovakva posebna ovlašćenja i njihove interakcije propisuju se posebnim dokumentima unutar IT sektora. Kad su u pitanju osobe koje se bave bezbednošću, u IT centralne banke urađena je podela na administratore bezbednosti (zaposleni u odeljenju za infrastrukturu) i savetnike bezbednosti koji se bave strategijama i politikama, zaposleni pri samom kabinetu rukovodilaca. Ovako se dele upravljačke i kontrolne funkcije od operativnih, i obezbeđuje da se izbegne sukob interesa. Na tu temu donose se pravila i preporuke u skladu sa standardima i najboljom praksom. U trenutku kad cela organizacija sazri za integrisanu bezbednosnu funkciju, poslovi grupe se podižu na nivo banke, što je standardom predviđena organizacija.

Jedno od pravila koje se poštuje kad su na primer u pitanju preklapanja bezbednosnih domena je da administrator operativnih sistema ne može ujedno biti i administrator sistema bezbednosti, ili upravljanja logovima.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 3.5.**

5.6. Logička bezbednost – Vreme

Nakon što je u prethodnom sloju opisan koncept zaštite nad životnim ciklusom, logički nivo mora definisati i životne cikluse samih bezbednosnih rešenja. Ovde se zahteva da se definiše kako se bezbednosna rešenja realizuju u vremenu, odnosno definiše se svojevrsni kalendar (koji će se popuniti konkretnim podacima na narednim slojevima) gde je navedeno kad počinju da se primenjuju, koliko traju, kakva je frekvencija primene i koji su uslovi za njihov prestanak.

Definisanje praćenja vremenskih odrednica je bitno da se obezbedi pokrivenost procesa zaštitom, kao i da se mere zaštite definišu u vremenskim okvirima (registracija, sertifikacija, logovanje na sistem, upravljanje sesijama itd.)

U sektoru za IT centralne banke, ovaj korak u projektovanju je jako važan, zato što ima veliki broj uređaja, servisa, programskih rešenja, i ovde dolazi do izražaja razuđenost arhitekture. Ovaj deo treba analizirati sa velikom pažnjom, jer se upravo ovde definišu sve vremenske međuzavisnosti poslovnih procesa i njihove pokrivenosti bezbednosnim rešenjima. Jedan od pristupa je da se krene od poslovnih procesa, i to prvo od upravljanja ljudskim resursima, te se, jedan po jedan analiziraju s obzirom na korištene resurse, a samim tim i primenjenu zaštitu. Izlazi iz ovakve analize mogu biti:

- Tehnologije odnosno servisi koje ne koristi nijedan poslovni proces
- IKT servisi koji nisu pokriveni zaštitom, ili ne prate standarde (npr. prijavljivanje na sistem ne prati promene u AD odnosno IM)
- IKT servisi koji funkcionišu nezavisno (nisu vezani ni na jedan kontrolni mehanizam i ažuriraju se ad-hok)
- IKT servisi na koje se ne primenjuju zakrpe ili ne postoji kontrolisan proces za to
- Poslovni procesi koji nisu pokriveni zaštitom tokom celog životnog ciklusa

Drugi važan korak je da se proveravaju ugovori i vremena održavanja odnosno isteka garancije, te vremena trajanja pojedinih sertifikata, protokola, dokumenata.

Na kraju, ovde je bitno i praćenje tehnoloških inovacija kojima se zamenjuju stara rešenja, i pravovremeno planiranje novih. Ovo je posebno važno za finansijski sektor, budući da postoje kako međunarodni standardi i preporuke (PCI DSS, preporuke ECB, preporuke BIS), tako i lokalni propisi kojima se reguliše oblast bezbednosti.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 3.6.**

6. Fizička bezbednost

Nakon definisanja logičkog sloja, sve što je tamo definisano prevodi se na fizički sloj. Na fizičkom sloju informacije se realizuju kao podaci, a bezbednosni servisi kao bezbednosni mehanizmi. Drugim rečima, ovde dizajner arhitekture predaje posao u ruke konstruktora. Konstruktor je neko ko će uzeti logičke opise i crteže iz prethodne faze i na osnovu njih predložiti tehnološki model koji će se koristiti za izgradnju „građevine“. Zadatak konstruktora je zapravo da prvo izabere, a zatim i sklopi u celinu konkretne fizičke elemente, koji će dati život logičkoj konstrukciji i napraviti pravu konstrukciju koja funkcioniše. To predstavlja fizički sloj bezbednosne arhitekture.

Na prelazu sa logičkog na fizički sloj već se oblikuje prava vrednost SABSA arhitekture, tu je već vizualizovana strategija: mapiranje poslovnih ciljeva IT ciljevima. Zato je SABSA poznata i kao poslovni pristup „*business approach*“. Dobar prikaz kako se od definicije poslovne strategije stiže do konkretnih bezbednosnih proizvoda i alata, daje **Slika 1a**.

Konkretno, kad govorimo o poslovnim informacionim sistemima, kao što je ovde upravo reč, i kad dođemo do faze postavljanja fizičkog sloja arhitekture, potpuno smo oslonjeni na ono što je urađeno u fazi dizajna (a na osnovu definicija iz prethodnih slojeva). Dizajner je taj koji mora da obezbedi sveobuhvatan skup logičkih apstrakcija koje će pokriti poslovne procese i informacije, i to na način da opiše bezbednosne servise koji treba da budu primenjeni. Ovo je vrlo važno da bi se odredio dobar bezbednosni mehanizam. Pored rizika da mehanizam ne pokrije sve što je u opisu servisa, postoji i druga opasnost, a to je da mehanizam pruži „previše“, što može bespotrebno ometati poslovni proces, onemogućiti neke njegove funkcije, i na kraju, ponekad uzrokovati i zaobilaženje bezbednosnog mehanizma.

Dakle, u ovoj fazi se dizajnirani bezbednosni servis prevodi u konkretno bezbednosno rešenje, u model koji će opisati trenutno aktuelne tehnološke modele, i dati konkretnu specifikaciju karakteristika njegovih komponenti. Ovde se logički koncept prevodi u termine fizičkih mehanizama, konkretnih rešenja i uređaja koji treba da obezbede realizaciju dizajniranih servisa.

6.1. Fizička bezbednost – Imovina

Da bismo odgovorili na pitanje „šta“ na fizičkom nivou, odnosno definisali fizičko dobro koje se štiti, potrebno je da napravimo specifikaciju poslovnog modela podataka. Podsećanja radi, na logičkom sloju su to bile informacije, a sad je potrebno uočiti konkretne podatke, nosioce informacija, odnosno modele podataka koji grade te informacije. Ovde se već vidi jasan prelazak na IT terminologiju.

Analiza postojeće strukture podataka može se pokazati većim poslom nego što se na prvi pogled očekuje. Naime, model podataka se postavlja pri projektovanju IS, a zatim neretko i dograđuje, dodaju se nove relacije i uslovljenosti. Savremeni poslovni zahtevi, otvaranje prema spoljnom

svetu, razmena informacija između korporacija, ali i sa fizičkim licima, pa i preko globalnih mreža, doneli su nove izazove kad je u pitanju relacija između bezbednosti i modela podataka.

Pored šema, indeksa, pointera, relacija, restrikcija, sad imamo i sertifikate, digitalne potpise, ključeve za enkripciju, a i sama IKT infrastruktura poseduje baze podataka bezbednosnih mehanizama. Dakle, poslovni model podataka mora biti upotpunjen i bezbednosnim podacima: korisnička imena, lozinke, setifikati i dr. Bezbednosni podaci čuvaju se u repozitorijumima operativnih sistema ili odgovarajućih bezbednosnih rešenja, i predstavljaju ne samo mehanizme već takođe i objekte zaštite. (Npr. rukovanje lozinkama).

Osnovna karakteristika podataka je da se oni mogu prikupljati, obrađivati i čuvati , te s tim u vezi imaju i osobine kao što su tačnost, oblast važnosti i relevantnost, vreme čuvanja. Sve su to atributi koje definiše poslovna funkcija, ali je pomoć stručnjaka iz IT neophodna, jer zaposleni u poslovnoj funkciji jasnije vide informaciju, dok im je sam podatak ponekad suviše apstraktan. Ono što je takođe bitna osobina ove vrste pristupa (*business approach*), je da se daje novi pogled na problematiku, koji je u stvari najispravniji. Radi se o tome da se tradicionalan pogled na IKT zapravo svodi na opremu i servise, pa tako govorimo o mreži, serverima, aplikacijama, bez prave svesti da su to komponente koje ne postoje same radi sebe, već u svrhu obrade i čuvanja podataka. Arhitektura bezbednosti bavi se izgradnjom zaštite poslovnih podataka koji su osnov poslovanja.

U ovoj fazi potrebno je, dakle, sagledati organizaciju poslovnih podataka, njihove konkretne objekte, kao i rečnik poslovnih podataka (*metadata*, podaci o podacima).

Ukoliko bi organizacija imala kapacitete i volju da se ovom koraku posveti sa povećanom pažnjom, (odnosno da ima razumevanja za poslove unutar IKT da se ova analiza uradi detaljno), posao u ovoj fazi može da posluži i za svojevrsan redizajn baza podataka, smanjenje redundantnosti, povećavanje skalabilnosti i fleksibilnosti, pogotovo kod baza podataka koje su dizajnirane ranije, po zastrelim metodologijama i u prevaziđenim okruženjima. To je još jedan dokaz u prilog da je SABSA metodologija pristup koji pored definisanja bezbednosne arhitekture doprinosi i redizajnu i modernizaciji čitave IKT arhitekture, pa i optimizaciji procesa u organizaciji.

U slučaju centralne banke, podaci su zapravo najvredniji i najosetljiviji resurs. Možemo reći da je reč o dve vrste podataka: osetljivi i tajni podaci vezani za strateško odlučivanje u samom vrhu finansijskog sektora države i koji su obeleženi određenim stepenom tajnosti i statistički podaci čitavog finansijskog sektora koji su po prirodi transparentni, ali gde bi narušavanje poverljivosti, integriteta i dostupnosti predstavljalo štetu po reputaciju ne samo centralne banke već i finansijskog sektora u celini.

Poslovni model podataka pravi se po aplikativnim modulima za određene poslovne procese. To je metodologija za inicijalno prikupljanje podataka za ovu fazu. Nastale evidencije, osim za potrebe arhitekture bezbednosti dobra su osnova za više procesa: utvrđivanje tajnosti, definisanje

odgovornosti, upravljanje kontinuitetom poslovanja, kompletiranje projektne dokumentacije, upravljanje procesima itd. Nakon što se definiše poslovni model podataka, sporedna korist od ovog koraka je svakako i eliminisanje redundantnih šema, tabela i/ili istih podataka u različitim tabelama.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 4.1.**

6.2. Fizička bezbednost – Motivacija

Motivacija, odnosno odgovor na pitanje: *Zašto štitimo podatke*, daje se kroz dobro definisana pravila upravljanja rizikom i procedure. Šta to zapravo znači? Od prvog sloja pa nadalje, kolona motivacije u matrici je bila vezana za rizik i upravljanje rizikom. Nakon njihovog nabiranja na kontekstualnom sloju, preko procene rizika na konceptualnom, na prethodnom logičkom sloju definisane su opšte bezbednosne politike.

Budući da fizički sloj daje konkretizaciju logičkog modela, tako i kod rizika: opšte principe zacrtane politikama ovde pretačemo u konkretna pravila i procedure, usmerene na konkretne zahteve koji se iskazuju u procesu donošenja odluka.

Na ovom nivou dovoljno je definisati opšti okvir pravila u kom se organizacija kreće. Radne procedure i uputstva biće napisane u kasnijim koracima, bitno je da se definiše opšti okvir, kao i to koje procedure i uputstva treba da postoje. Templejti za operativnu dokumentaciju mogu se postaviti na ovom nivou.

Treba imati na umu da je bezbednosna arhitektura sama po sebi retko loša – koji god pristup da uzmemo smernice nas vode do sveobuhvatne zaštite onoga što je procenjeno kao rizik. Dakle, ono što može biti loše urađeno je upravo upravljanje rizikom.

Veoma bitno prilikom izrade ove dokumentacije je upravo da to ne bude samo „dokumentacija“ koja će formalno pokriti zahteve, već da se opišu i dokumentuju prakse koje su realne za implementaciju, a podržavaju propisane politike. Pravila takođe moraju biti odraz politike s jedne, ali i podrške radnim operacijama sa druge strane. Uvođenje spiska želja u pravila i procedure, ili prepisivanje principa koji su primenjeni negde drugde ili preporučeni u literaturi može imati za rezultat da se oni ne poštuju, što otvara bezbednosne šupljine, a istovremeno poništava sav uloženi trud.

U slučaju centralne banke prvi koraci u implementaciji bezbednosti urađeni su upravo sledeći najbolje prakse i opšteprihvaćene modele. Slabosti tog pristupa pokazale su se u redundantnosti kontrola u pejedinim tačkama, ali i neočekivanim šupljinama koje su se pokazivale tek prilikom incidenta. Jedan veliki i specifičan sistem kao što je centralna banka, samim tim što se radi o jedinstvenoj organizaciji, ne može preslikavati opšte, standardno rešenje. Prvi korak u izgradnji autentičnog rešenja bio je u prihvatanju smernica ECB i razmeni iskustava sa drugim centralnim

bankama. Pokazalo se da „best practice“ pristup, bez pravog upravljanja rizikom ne može dati zadovoljavajuće rezultate. Isprva, procedure su formalno opisale procese, ali pravo stanje bezbednosti nije se moglo lako utvrditi, jer su kriterijumi bili postavljeni na osnovu najbolje prakse, a ne realnih poslovnih zahteva. To je bio i jedan od pokretača ideje za izradu arhitekture, pa su se iskustva sličnih organizacija primenjivala s obzirom na aktuelno stanje a ne na *copy-paste* principu, što je bio ključni korak.

Na ovom sloju definiše se potreba za procedurama definisanim krovnim dokumentom, politikama (definisane na logičkom sloju). Nepridržavanje politika je rizik, a pravila i procedure proisteći će upravo iz analize rizika i predloga za njihovo umanjeње. Svakako, procedure su postojale i ranije, ali ovde se pruža prilika da se napravi i povratna veza, da se svakoj proceduri pridruži jedan ili više rizika koji se smanjuju njenom primenom.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 4.2.**

6.3. Fizička bezbednost – Proces

Kako implementirati zaštitu na fizičkom nivou, definišu upravo bezbednosni mehanizmi u širem smislu. Na prethodnom sloju odredili smo koji su to bezbednosni servisi, i sad je vreme da se oni prenesu u konkretne izvedbe na postojećim aplikacijama, srednjim slojevima, mrežnim komponentama – da definišemo mehanizme zaštite.

Konkretno, ovde se opisuju i definišu mehanizmi kao što su: enkripcija, kontrola pristupa, digitalni potpisi, skeniranje na viruse, sprečavanje oticanja podataka, filtriranje saobraćaja, filtriranje elektronske pošte, kao i konkretne aplikacije, okruženja i serveri potrebni da se realizuju ovi mehanizmi. Upoznavanje zaposlenih sa pojmovima i pravilima bezbednosti, podizanje svesti i obuka korisnika takođe je važan bezbednosni mehanizam. Svi bezbednosni mehanizmi moraju postojati pre ovog koraka definisani i opisani u takozvanoj **bazi podataka bezbednosnih mehanizama** [1].

Dok su bezbednosni servisi na logičkom sloju predstavljali samo logički prikaz servisa koji su potrebni, bez ulaženja u njihove međusobne odnose, mehanizmi na fizičkom nivou traže veću pažnju. Prvo je važno primetiti da preslikavanje između servisa i mehanizama nije jedan na jedan. Često jedan mehanizam pokriva više od jednog servisa, a moguće su i varijante da je za realizaciju jednog servisa potrebno više mehanizama. Stoga je važno stalno imati na umu opseg pokrivanja određenim mehanizmom (*scope*) , i izbeći preklapanja kao i nepodržane servise. Sa druge strane, broj tipova bezbednosnih mehanizama treba minimizovati, da bi se umanjila kompleksnost koja je rizik sam od sebe, a što je i jedan od ciljeva ovog pristupa.

Pritom, važno je imati na umu da servise, a samim tim i mehanizme determiniše potreba za zaštitom poverljivosti, integriteta i raspoloživosti poslovnih podataka, što je opet u neraskidivoj vezi sa modelom poslovnih procesa (vertikala matrice).

Uzevši u obzir ITIL terminologiju, mehanizmi zaštite koji su ovde definisani deo su takozvanog operativnog upravljanja, tj. rasporeda poslova i upravljanja događajima i incidentima (*Job Scheduling, Event&Incident Management*).

U slučaju centralne banke bezbednosni mehanizmi su uspostavljeni i pre nego je sama bezbednost prepoznata kao uređena oblast u IT. Razlog tome je opredeljenje institucije da se poštuju najviši standardi u poslovanju, kao i svest o postojanju rizika od gubitka podataka ili narušavanja reputacije čak i kad se to nije formalno i proceduralno uređivalo. Razvoj funkcije bezbednosti u IT doprineo je da se postojeći mehanizmi analiziraju, da se identifikuju uska grla, dvostruke kontrole i nebranjene tačke.

Osnovna karakteristika bezbednosnih mehanizama implementiranih u centralnoj banci je da su usmereni ne samo zaštititi osetljivih podataka i informacija, već i pojačavanju subjektivnog osjećaja sigurnosti za zaposlene, rukovodioce, ali isto tako i ceo bankarski i finansijski sektor. Zato je odgovornost u implementaciji ovih mehanizama u centralnoj banci velika, budući da prevazilazi granice organizacije.

Nakon implementacije tradicionalnih bezbednosnih mehanizama, centralna banka implementirala i savremene, višenamenske mehanizme kao što su monitoring mreže, SIEM i slično. Novi pristup i prihvatanje novih tehnologija logično dolazi prateći tendencije i razvoj infrastrukture ali i pretnji.

Sve to nalazi se u **Katalogu kontrola**, koji se stalno dopunjuje, i koji predstavlja bazu podataka bezbednosnih mehanizama.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 4.3**.

6.4. Fizička bezbednost – Ljudi

Nakon što su na logičkom nivou pobrojane funkcije i profili zaposlenih, na fizičkom će biti reči upravo o zaposlenima kao korisnicima IKT sistema. Preciznije rečeno, ova faza opisuje konkretne korisničke interfejsa, kao mesto gde se „susreću“ korisnici i sistem, i gdje se implementiraju bezbednosni mehanizmi.

Kad je reč o korisničkim interfejsima, potrebno je zapravo definisati kolika je interakcija (pa time i zavisnost) između čoveka i sistema, šta sve sadrže ekrani, kako se oni menjaju i prilagođavaju s obzirom na korisnička ovlašćenja. Definišemo ko će biti obuhvaćen sigurnosnim mehanizmima. Pored toga, ovde se definišu svi sistemi kontrole pristupa.

Konkretno, posmatrajući servise, ove informacije treba da budu raspoložive servis desku, i osnova rešavanja zahteva i upravljanja problemima, jer upravljanje problemima u najvećem broju slučajeva počinje nekom prijavom korisnika, i to treba da bude ulazni podatak ka svim

ostalim podacima o korisniku, odnosno resursima koje koristi i poslovnim procesima na koje utiče svojim radom.

Sa druge strane, podrška korisnicima, i kroz servis desk i kroz bezbednosne mehanizme, zapravo je ključni smisao definisanja ove faze.

U slučaju centralne banke, zahvaljujući prvenstveno ITIL principima, prihvaćen je servisni pogled, i podrška korisnicima kao centralna tačka. Korisnik je stavljen u centar, i interfejsi su unificirani i standardizovani koliko god je to moguće.

Način opisivanja radnog mesta, i način pisanja procedura prema sistemu kvaliteta usvojenom u banci učinili su da se korisnik i proces već pri definiciji profilisu tako da se mogu sa priličnom tačnošću kreirati aplikativne role prema zahtevu radnog mesta.

Procedurama je uređeno da se na svaki sistem za koji je to moguće korisnik loguje AD nalogom, te da su prava i ovlašćenja definisana rolama. S obzirom na to, svaki izvršilac funkcije ima interfejs prilagođen svojim ovlašćenjima.

Sistemi kontrole pristupa koji su u upotrebi su: politika dodele korisničkog imena i odabira lozinke, jednokratno logovanje, RBAC itd, dok se u pojedinim slučajevima koriste i dodatne kontrole fizičkog pristupa, personalizovane kartice i slično. Bitno je da se identifikuju bezbednosni elementi svakog korisničkog interfejsa, i da se ta evidencija ažurira sa pojavom svake nove aplikacije ili izmenom postojeće. Ovo se postiže tako što se ovaj korak uvrsti u proces upravljanja aplikativnim projektom i u proces upravljanja promenama.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 4.4.**

6.5. Fizička bezbednost – Lokacija

Kada se na fizičkom nivou postavi pitanje gde, misli se zapravo na ukupnu infrastrukturu: mreže, opreme i platforma na kojima se odvijaju poslovni procesi, gde su pohranjeni i kuda se kreću podaci, i shodno tome implementira zaštita. Ovde se konkretno specificira lokacija (kako logička tako i fizička) svakog hosta, svakog čvora, svaki komad hardvera u mreži je važno locirati i definisati da li se, i pomoću kojih konkretnih mehanizama štiti. Lokacija komponenti informacionog sistema usloviće i lokaciju i konkretnu izvedbu mehanizama zaštite. Ovde se definiše i gde će se nalaziti bezbednosna arhitektura, odnosno njeni elementi, ovde praktično proveravamo da li smo dobro definisali bezbednosne domene na prethodnom sloju, što će se videti kroz odgovor na pitanje da li je predloženim mehanizmima sve pokriveno, te da li ima nepotrebnih preklapanja.

Najbolje je da izlaz iz ove faze budu dijagrami, kako topologije mreže, tako i pojedinih njenih delova, sa detaljnim opisom čvorova i konfiguracija. Za sav hardver mora da postoji podatak: koliko, kog tipa i gde.

U slučaju centralne banke infrastruktura mreže se prati kroz nekoliko kontrolnih mehanizama, a u planu je i uspostavljanje NOC i SOC kontrolnih tačaka. Infrastruktura bezbednosti je izgrađena na tehnologijama po preporukama najbolje prakse, ali i po zahtevima poslovanja koji definišu kritičnu infrastrukturu, pa samim tim i mehanizme njene zaštite.

Za mrežnu i serversku infrastrukturu postoje dijagrami koji prikazuju topologiju, a postoji ažurna evidencija infrastrukture i to po tipu i nameni. Definisane su i propusnosti određenih komunikacionih kanala i kapaciteti servera i storidža. Ustanovljeno je i nešto kao „lična krta“ svakog hosta, uređaja i linka

Naredni korak je procena optimalne redundanse, odnosno unapređenje postojeće procene, budući da se primenom virtualizacije ova oblast značajno unapredila u potencijalima.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 4.5.**

6.6. Fizička bezbednost – Vreme

Upravljanje vremenom je aktivnost koja treba da bude definisana već pri dizajnu procesa i servisa i upravljanju njima. Kao i u ostalim segmentima, tako i ovde, arhitektura bezbednosti ne može da se posmatra izolovano, već se uklapa u definiciju postojećih aktivnosti.

Uspostavljanje ovog segmenta odgovara na pitanje: Kad pustiti u rad kontrolne strukture? Kad će i kojom dinamikom oni biti ugrađivani u procese? Koji su vremenski intervali za provere? Uspostavljanjem vremenskih odrednica za bezbednosne mehanizme, proverićemo i koliko su dobro definisani životni ciklusi procesa i servisa, šta je zaista kritično i da li imamo vreme koje nije pokriveno podrškom.

U slučaju centralne banke osnovno je da se uspostave kontrolni mehanizmi za proveru rada bezbednosnih rešenja. Jedan od primera za ovo je i kontrola redovnog slanja logova na SIEM, i notifikacije prilikom prestanka slanja logova. Takođe, implementirane su razne vrste alerta u slučajevima kad se bezbednosni mehanizmi isključe.

Što se tiče praćenja servisa i usklađivanja rada servisa sa radom bezbednosnih i kontrolnih mehanizama, u toku je implementacija SLA i OLA, gde će se i formalno definisati intervali podrške.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 4.6.**

7. Komponente bezbednosti

Nakon što se na prethodnom sloju izgradila konačna slika sa svim elementima koje će arhitektura bezbednosti imati i definisani su konkretni mehanizmi koji će se koristiti, dolazimo do trenutka kad se govori o realnim komponentama – ovo je pogled „trgovca“, koji za svaki naš projektovan element, odnosno mehanizam zaštite, ima određeni proizvod ili servis. Pogled prodavca obuhvata sve ono što su hardverske komponente, softverske komponente, interfejsi, specifikacije i standardi. Moderne tendencije u IKT industriji brišu znak jednakosti između reči „uređaj“ i „rešenje“, jer je sve manje modernih bezbednosnih rešenja u obliku fizičkog proizvoda koji se pakuje u „kutiju“ ili rek. Ponekad su to virtualne mašine, ili čak samo instalacije na poseban ili neki od postojećih servera. Ponekad je to naprosto servis, nastao integracijom više hardverskih i softverskih komponenti i aktivnosti. Zato je prethodni, fizički sloj veoma bitan, jer najviše što može da se uradi „u kući“ je da se dobro definišu fizičke osobine i mehanizmi zaštite.

Komponente će se nabaviti na tržištu, i jedino što možemo u ovoj fazi je da upoređujemo definicije i potrebe koje smo postavili na prethodnom sloju, sa karakteristikama komponenti koje se nude na tržištu. Važna aktivnost ovde je i integracija pojedinih komponenti, kako jednih sa drugima, tako i sa već postojećom, i planiranom infrastrukturom.

U konkretnom slučaju, kad govorimo o centralnoj banci, ovaj sloj realizuje se kroz proces nabavke na tenderu (ovo je obavezan deo za instituciju, tržišne organizacije su reklasirane od ovakvog načina nabavke i mogu se u startu odlučiti za vendora i proizvod), te je pisanje tenderske dokumentacije najosetljiviji deo. Postavljanje bezbednosne arhitekture pomoći će upravo i kvalitetnijoj izradi tenderske dokumentacije, jer pruža sistematski pristup, i ne dozvoljava da se zanemare osnovni elementi, a to je ono zbog čega se sve i radi – podaci koji treba da se zaštite.

Osnovno u postavljanju tenderskog zahteva je da se uz detaljne karakteristike zahtevanog proizvoda traži i tim integratora koji će novo rešenje integrisati sa postojećom infrastrukturom, i rešenjima planiranim za buduće nadogradnje. Dakle u timu integratora treba da se pronađu osobe koje su orjentisane na softver, na hardver kao i stručnjaci za servise. Postojanje arhitekture ovde dobija na značaju.

7.1. Komponente bezbednosti – Imovina

U ovom koraku definišemo ono što je u izvornom obliku zapravo jedino i vidljivo iz IKT sektora organizacije, a to je detaljna struktura podataka (šeme baza podataka sa opisima svakog podatka i sintaksnim pravilima, ali i svi repozitorijumi podataka, čak i ručno rađeni spiskovi koji imaju uticaj na poslovne procese) sa jedne, i detaljne kritične hardverske komponente (ovde su konkretni IT proizvodi i komponente, npr. memorijske jedinice, serveri, na kraju i procesori) s druge strane. Takođe, poslovna aplikacija kao automatizovan niz aktivnosti predstavlja komponentu. Dakle, kad kažemo imovina na ovom sloju, mislimo upravo na najmanje jedinice

IKT proizvoda - šeme baza podataka sa opisima i pravilima, aplikacije, servere, koje su u opsegu rešenja zaštite.

U slučaju centralne banke koji se razmatra radi se o velikim bazama podataka koje sadrže puno statističkih podataka iz različitih izvora. Baze podataka su razvijane na različitim tehnologijama, ali se radi o „enterprise“ proizvodima koji su standardni, dokumentovani i podržani. Repozitorijumi vezani za šeme baza podataka se lako dobijaju raspoloživim alatima. Sa druge strane, projektna dokumentacija i uputstva omogućuju detaljan uvid u strukture podataka koje se razmenjuju sa drugim organizacijama i pravila koja važe za provere tih podataka. Hardverske komponente vidljive su u specifikacijama i postignut je visok nivo standardizacije opreme s obzirom na namenu (radna stanica tip 1,2,3, serveri prema nameni, itd).

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 5.1.**

7.2. Komponente bezbednosti – Motivacija

Zašto postavljamo komponente bezbednosti i zaštite? Jedan od glavnih motiva su uspostavljeni standardi bezbednosti na koje smo se obavezali u cilju pouzdanog obavljanja aktivnosti i postizanja poslovnih ciljeva. Da bi formalizovali ovaj korak tu su alati i proizvodi za upravljanje operativnim rizikom, registri rizika i alati za nadziranje i izveštavanje o rizicima. Takođe, ukoliko postoji kontinuitet poslovanja kao uspostavljen proces, alati će se takođe naći ovde. U protivnom, ovaj korak treba da naglasi potrebu uspostavljanja upravljanja kontinuitetom poslovanja kao neophodne karike za buduću arhitekturu preduzeća.

U centralnoj banci usvojene su Politike bezbednosti, koje se odnose na instituciju u celini i za čije sprovođenje su nadležni ne samo IT sektor već i Odbor za bezbednost (telo na nivou najvišeg rukovodstva), organizacioni deo koji se bavi ljudskim resursima, kao i svaki rukovodilac. Međutim, politike predlaže, kontroliše, revidira upravo IT sektor, što se pokazalo kao najbolje rešenje i što potvrđuje osnovnu tezu ovog rada da se sa projektovanjem IKT bezbednosti treba krenuti iz IKT sektora. Pored konkretnih politika, ovde se definišu i svi ostali bezbednosni standardi na koje se oslanja organizacija. Tu su takođe i standardi proizvođača pojedinih rešenja.

U konkretnom slučaju upravo nakon što je IT sektor predložio Politiku bezbednosti i krenuo u procenu rizika, pokazala se potreba za uspostavljanjem i formalnim definisanjem upravljanja kontinuitetom poslovanja u banci kao celini. Pored ISO2700 standarda, za koji se banka načelno odlučila da ga se pridržava (bez odluke o sertifikovanju za sada), postoji niz standarda koji su vezani za finansijsko poslovanje i slabilnost (Basel2, Basel3, PCI DSS i sl.) a koji imaju uticaj na primenjena bezbednosna rešenja.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 5.2.**

7.3. Komponente bezbednosti – Proces

Odgovor na pitanje kako realizovati komponente bezbednosnih rešenja krije se upravo u bezbednosnim proizvodima i alatima i načinima njihovog korišćenja. Na primer, tu se navodi kako se vrši administracija korisnika, kako se radi bekap, kako se prate logovi i nadziru bezbednosni događaji i slično. Ovde je, pored samih procesa i alata zaštite bitno definisati i sam proces nabavke. Hardverske i softverske komponente koje se nabavljaju zajedno sa standardima koji su ugrađeni treba da pruže sliku konkretne realizacije zaštite.

Izlaz iz ovog koraka je lista sa opisima i specifikacijama tehnologija, proizvoda i alata koje će biti izabrane, zajedno sa detaljnim uputstvom za bezbednosni tim o tome kako, zašto, gde i kada trebaju biti korišćeni.

Bezbednosni proizvodi i alati u centralnoj banci raspoređeni su po perimetru mreže po principu „zaštite u dubinu“. Isto tako, uvođenjem procesa procene rizika i određivanja bezbednosnih zahteva na osnovu rizika, pokazala se potreba za dodatnim tehnologijama. Treći pokretač nabavke novih rešenja je revizorski nalaz. Sve ovo uklapa se u koncept izgradnje bezbednosne arhitekture, i naslanja se na prethodni sloj gde su definisani mehanizmi. Pokazalo se da su neki mehanizmi već pokriveni komponentama, ali u određenom broju slučajeva ta pokrivenost nije potpuna, te se pokazala potreba za definisanjem novih mehanizama (na primer, SIEM pruža statičku analizu istorijskih podataka, pa je potrebno da se dopuni *sand-box* mehanizmom za otkrivanje malvera na osnovu ponašanja saobraćaja u mreži).

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 5.3.**

7.4. Komponente bezbednosti – Ljudi

Dok smo na prethodnom sloju definisali interfejse za komunikaciju zaposlenih sa sistemom, ovde se bavimo njihovim konkretnim ulogama, opisima poslova, identitetima, rolama, svim onim alatima koji uređuju oblast upravljanja personalom i pravima pristupa. Tu su i ACL (liste kontrola pristupa), kao i logovi akcija pojedinaca na sistemu. Takođe, ovde se definiše ko zapravo definiše komponente (to su identiteti, uloge, kontrole pristupa), odnosno kako se komponente bezbednosti vezuju za ljude, odnosno njihove aktivnosti i uloge u procesu.

Postoje metodologije i alati koji omogućuju da se ovaj korak napravi kvalitetno, a u velikim i razgranatim organizacijama ovo može predstavljati zaista složen zadatak. Povezivanje opisa radnog mesta sa kadrovskom evidencijom i sve to sa AD je jedan od dobrih pristupa. Međutim, primenjiv je samo na Windows OS, i ne može se posmatrati kao sveobuhvatno rešenje, već je potrebno napraviti interfejse koji će omogućiti primenu principa na sve korisnike.

ACL je starija tehnologija, i u novije vreme biva zamenjena RBAC tehnologijama koje doprinose smanjenju kompleksnosti, i omogućuju bolje performanse ali i jednostavnije

upravljanje pravima i ovlašćenjima. U svakom slučaju, izlaz iz ovog koraka su definisani opisi poslova, identiteti, liste prava pristupa, nivoi ovlašćenja, liste mogućih akcija na sistemu.

U centralnoj banci postoji sprega između kadrovske evidencije i elektronskog identiteta zaposlenih. Ona je realizovana kroz Identity Manager, koji je interfejs između evidencije ljudskih resursa i AD, odnosno sličnog direktorijuma digitalnih identiteta na ostalim, new-windows sistemima.

Liste pristupa (ACL) se još koriste na nekoj mrežnoj opremi i starijim aplikacijama, ali je nastojanje da se gde god je to moguće pređe na RBAC. Aplikativni interfejsi, kao što je objašnjeno ranije, omogućavaju jednostavno definisanje radnog okruženja, prava i ovlašćenja na osnovu definisanih rola.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 5.4.**

7.5. Komponente bezbednosti – Lokacija

Budući da je na prethodnom sloju definisana mrežna i hardverska infrastruktura, ovde će se samo specificirati konkretni čvorovi, njihove IP adrese i ostali identifikatori koji jednoznačno definišu položaj uređaja i/ili procesa odnosno servisa u mreži, šta su zapravo tačke u kojima će biti implementirane komponente zaštite. Definišu se i protokoli i adresne šeme. Kad se zna gde će se implementirati komponente bezbednosti može se govoriti i o njihovoj integraciji, i dokumentovati da se planirani mehanizam može realizovati definisanom komponentom. Ukoliko se radi o mehanizmima koji imaju lokalne (jedan LAN), ili namenske (endpoint, server, mreža) instance, definiše se koji domen pokriva određena komponenta.

U centralnoj banci postoje ili su u planu različiti alati za monitoring mreže, koji ujedno i daju prikaz topologije, i analitiku po različitim kriterijumima. To olakšava identifikaciju tačaka u koje se postavljaju bezbednosna rešenja, i to ne samo tehnička, već i organizaciona i upravljačka, a na način da se obezbedi projektovana zaštita ne ugrožavajući performanse.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 5.5.**

7.6. Komponente bezbednosti – Vreme

Implementacija bezbednosnih komponenti, osim po lokacijama, mora biti precizno utvrđena i u vremenu. To je odgovor na pitanje *kad* na sloju komponenti bezbednosti. Vremenske odrednice ovde definišu ne samo vreme početka implementacije bezbednosnih komponenti i rokove, već i vremenske rasporede za integraciju tih rešenja. Ovo je vrlo važno jer ukoliko se komponente prebrzo puštaju u rad jedna za drugom, može da se desi da se integracija ne uradi dobro, ili da monitoring informacija koje rešenje nudi bude izvršen na neodgovarajući način, te da se ostane bez osnovnih informacija koje komponenta zapravo mora da pruži.

Primer loše integracije usled kratkih rokova bio bi na primer implementacija uređaja za filtriranje saobraćaja na mreži pre detaljne analize procesa koji se izvršavaju preko određenih portova, te slučajno onemogućavanje regularnih poslovnih aktivnosti kroz mrežu pokušajem da se filtrira neki neodgovarajući sadržaj. Drugi primer je uvođenje SIEM (*Security Incident and Event Management*) sistema bez prethodno razvijenog upravljanja logovima i njihovog potpunog razumevanja. Posledica je da se „događaji“ generisani korelacijama logova i potencijalni bezbednosni incidenti kreiraju samo na osnovu uputstava i najbolje prakse, te da sadrže mnogo lažno pozitivnih upozorenja. IDS/IPS sistemi takođe zahtevaju postepenu integraciju, a istovremeno, njihovo postojanje je preduslov za implementaciju sistema za monitoring mreže i detekciju. Vremenska komponenta bezbednosti je veoma važna u upravljanju incidentima.

Budući da centralna banka ima kompleksnu i razgranatu računarsku mrežu i obilje rešenja i funkcionalnosti, te da je opredeljenje i obaveza da se prate poslednji standardi iz oblasti kako razvoja IKT, tako i bezbednosnih odgovora na savremene pretnje, veoma je važno da se usled loše planiranog vremena ili neuspešne integracije rešenja dovede u pitanje funkcionisanje poslovnih funkcija.

Obaveza javne nabavke dodatno usložnjava problem integracije, budući da ne postoji mogućnost da se planski kombinuju komponente istog proizvođača. S tim u vezi, bitno je da tehničke specifikacije sadrže jasne i nedvosmislene zahteve za integracijom novog rešenja sa postojećom arhitekturom. Vremenski prozori za rad bezbednosnih mehanizama zavise od radnog vremena korisnika servisa, i kreću se od nekoliko sati do 24 sata dnevno. Razvojem NOC i SOC funkcija omogućiće se njihovo neprestano nadziranje i definisanje dežurstava („*on duty*“).

Predlog dokumenta koji predstavlja izlaz iz ovog koraka dat je u **prilogu 2, Sekcija 5.6**.

8. Operativno upravljanje bezbednošću

Kad je jednom završena izgradnja, kad arhitekta, dizajner i konstruktor završe i predaju „građevinu“ u upotrebu, potrebno je da se neko bavi njenim održavanjem tokom životnog ciklusa. Ovo je posao operative, koja se zapravo u čitav proces aktivno uključuje još ranije, negdje na početku definisanja logičke infrastrukture (Slika 2.). Zato kažemo da je ovo pogled menadžera objekta, odnosno servisnog menadžera. To je posao čiji je opis vođenje brige o svim operacijama nad izgrađenim, o različitim servisima koji se pružaju, održavanju, kao i monitoringu toga kako dobro se zadovoljavaju svi zahtevi koji su pred izgrađeno postavljani u toku prethodnih faza analize potreba, projektovanja i implementacije. Okvir za ovo se još zove i „**arhitektura upravljanja servisima bezbednosti**“ (eng. *service management security architecture*).

U širem smislu, kad se posmatra informacioni sistem u celini, upravljanje servisima se bavi klasičnim operacijama na sistemu, svim operacijama na ukupnom sistemu, kroz praćenje,

održavanje i unapređivanje njihove operativnosti, pouzdanosti i svrsishodnosti. Ovde je pažnja usmerena samo na bezbednosne aspekte tog posla, ne gubeći iz vida činjenicu da se radi o funkcionalnostima, odnosno poslovima izdvojenim iz jedne veće slike, u svrhu njihovog opisivanja i sagledavanja, a ne da bi se na bilo koji način implicirala mogućnost da bezbednosne operacije postoje same za sebe.

Dakle, završni sloj prema SABSA matrici je servis za upravljanje bezbednošću sistema, i bavi se tekućim održavanjem implementiranih bezbednosnih rešenja i mehanizama u produkcionom okruženju jednog informacionog sistema. Odgovori na pitanja iz matrice zapravo su uslovi koji moraju biti definisani u trenutku kad se bezbednosna rešenja i mehanizmi puštaju u produkcionu rad.

Sa druge strane, ako pogledamo prikaz konkretizacije rešenja od poslovne strategije do proizvoda, **Slika 1a**, prednosti slojevitog pristupa ovde najbolje dolaze do izražaja: umesto da se za svaki proizvod i alat ponuđen na tržištu polazi iz početka od poslovnih potreba, one su već definisane na prethodnim slojevima i razrađene kroz procene rizika. Vrlo lako uočavamo da li je nešto što nam se nudi, ili imamo nedoumicu potrebno ili ne. Svaka promena u poslovnim zahtevima i ciljevima ukoliko se ažurno sprovede kroz dokumentaciju bezbednosne arhitekture vodiće do proizvoda kojim se realizuje zaštita, i moći ćemo da zaključimo da li vid zaštite za taj poslovni zahtev već postoji ili mora da se izvrši nabavka ili dogradnja.

8.1. Operativna bezbednost – Imovina

Odgovor na pitanje *šta* na operativnom nivou je u stvari ukupan bezbednosni resurs, a to je upravljanje isporučivanjem servisa, odnosno drugim rečima obezbeđivanje operativnog kontinuiteta bezbednosne implementacije. To znači da je potrebno pružiti uveravanje da će se održati neprekidnost rada bezbednosnih mehanizama, kao i stabilne, visoke performanse u zaštiti operativnih poslovnih podataka i informacija. Prakse koje će obezbediti takav način pružanja usluge predmet su ovog koraka. Pored politika kao krovnog dokumenta potrebno je imati definisane, i u praksi potvrđene operativne procedure i uputstva, garancije proizvođača i vendora, ugovore, definisano i dokumentovano praćenje procesa.

Okvir za operativni kontinuitet bezbednosti obuhvata: proces prikupljanja poslovnih zahteva, klasifikacionu šemu informacija, proces ili program upravljanja kontinuitetom poslovanja, proces upravljanja informacionom bezbednošću, proces upravljanja integracijama u IS, proces upravljanja bezbednošću baza podataka, proces upravljanja integritetom softvera, proces upravljanja integritetom i bezbednošću upravljačkih procesa i bezbednosnih proizvoda i alata.

Na primeru IT sektora centralne banke koji se obrađuje nesumnjivo su prepoznati svi elementi okvira, ali se ne može reći da su svi i razvijeni u trenutku pisanja ovog rada. Na procesima upravljanja kontinuitetom poslovanja i na klasifikaciji se radi. Istovremeno, za sve infrastrukturne servise postoje detaljne funkcionalne specifikacije, plan implementacije,

definisani su koraci praćenja projekta od plana do penzionisanja pojedinog rešenja kroz sve faze implementacije i održavanja, a za svaki infrastrukturni, pa time i bezbednosni servis, redovno se radi pregled izvedenog stanja. Tako se obezbeđuje ne samo evidencija bezbednosnog resursa i identifikovanje njegovih procesa, već i stanje u svakom trenutku i praćenje dinaminke promena.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka za primer centralne banke dat je u **prilogu 2, Sekcija 6.1.**

8.2. Operativna bezbednost – Motivacija

Zašto se sve to radi, kao i kroz čitavu kolonu motivacije u matrici, odgovor je: rizik. Ovde već moramo imati konkretan i zaokružen proces upravljanja operativnim rizikom (procena rizika, monitoring i izveštavanje, analiza i na kraju tretiranje rizika) u smislu minimiziranja uticaja koji mogu izazvati prekid ili nepravilnosti u izvršavanju operacija.

Ovde će se naći i procesi kontrole i revizije bezbednosti, procesi izrade i održavanja politika, provere usklađenosti, procene ranjivosti, pretnji, penetraciono testiranje, i na kraju, izveštavanje nadležnog CERT.

Planiranje kontinuiteta poslovanja je logičan i prirodan nastavak rada na upravljanju rizicima, i ujedno cilj svake organizacije, te je zapravo i konačan cilj u određivanju motivacije. Pitanjima rizika, a samim tim i kontinuiteta poslovanja često se prilazi olako, čekirajući korake iz uputstava, standarda, literature. U stvarnosti se uvek ispostavi da je ovaj posao i teži, i dugotrajniji i teže razumljiv u važnim detaljima nego što se to na početku čini. Standard nije metodologija, samo postavlja zahteve, zato je važno imati razvijenu metodologiju upravljanja rizicima i razvijenu svest o važnosti među svim zainteresovanim stranama. Sa ispunjenjem tih preduslova plan kontinuiteta poslovanja će biti jasan i upotrebljiv.

U slučaju centralne banke okvir upravljanja operativnim rizicima je u trenutku pisanja ovog rada u procesu implementacije. To znači da su postavljeni principi, i da se u IT sektoru, kao i nekim sektorima koji se bave kritičnim poslovnim procesima već pristupilo upravljanju operativnim rizikom, što je iniciralo potrebu da se uspostavi i upravljanje kontinuitetom poslovanja na nivou cele organizacije, što je u toku. Oblast istraživanja je dokumentacija IT sektora, te će se procenjeni rizici koristiti u obimu u kom se tiču IKT procesa. Ekspanzijom IKT servisa vrlo je malo rizika koji nemaju uticaj i na IKT.

U **prilogu 2, Sekcija 6.2.** naveden je izlaz iz ovog koraka koji obuhvata postojeću dokumentaciju, kao i onu planiranu.

8.3. Operativna bezbednost – Proces

Kako sprovesti operacije vezane za bezbednost? Kako izneti procese vezane za bezbednost i upravljati njima? Tu je prvenstveno upravljanje i podrška sistemima, aplikacijama i servisima, izvršavanje specifičnih specijalizovanih operacija povezanih sa bezbednošću, kao što su administracija korisnika bezbednosnih rešenja, administracija sistema bezbednosnih rešenja, bekapi podataka, nadgledanje i praćenje bezbednosnih indikatora, procedure za reagovanje na incidente bezbednosti i nepredviđene događaje i slično.

Konkretno, ovde se ne barata sa postojanjem navedenih aktivnosti i njihovim nabranjanjem, već će se zapravo navesti precizno kako se vrši administracija korisnika, kako se radi bekap, kako se prate logovi i nadziru bezbednosni događaji i slično. Iz opisa procesa vezanih za bezbednost na operativnom nivou mora biti vidljivo da se operacije bezbednosti zaista sprovedu, da su jasne i međusobno povezane, te da su poslovni procesi pokriveni bezbednosnim procesima.

Pored upravljanja bezbednosnim događajima i incidentima tu je još i proces oporavka od pada, proces kontrole upravljanja promenama, proces upravljanja konfiguracijama, konfiguracije sistema kao što su IDS/IPS, SIEM, kao i sve operativne procedure vezane za pravila, PKI, ACL, bekap, logovanje, AV administraciju i slično.

Takođe, bitno je da se na operativnom bezbednosnom nivou jasno definiše uloga u nabavkama, u operativnom menadžmentu i upravljanju projektima.

U primeru centralne banke upravljanje bezbednosnim servisima je sve više uslovljeno poslovnim zahtevima, čemu je doprinelo usvajanje *Metodologije upravljanja informatičkim rizikom*⁶, gde se vrši procena rizika za projekte IT podrške poslovnim procesima i na osnovu toga pravi lista bezbednosnih zahteva i odgovarajućih bezbednosnih kontrola iz kataloga.

Definisano je upravljanje incidentima i u okviru toga incidentima bezbednosti, kao i postupanje u slučaju da bezbednosni incident uzrokuje nepredviđene okolnosti. Redundansa i bekap su obezbeđeni i proceduralno uređeni. Rad sa udaljene lokacije i oporavak od pada implementirani su za kritične funkcije, i postepeno će se, u skladu sa planiranim kapacitetima povećavati broj redundantnih tehnologija tamo gde to zahtevi bezbednosti i procenjeni rizik zahtevaju.

Upravljanje promenama je uređeno u skladu sa ITIL principima i primenjeno je i na bezbednosne servise. Upravljanje logovima i korelacija događaja obezbeđuju forenzički spreman sistem. Razvoj i implementacija novih servisa koje će nametati stalna trka „dobrih i loših momaka“ u kiber prostoru pokazuje da je program upravljanja i podrške definisan kao fleksibilan i skalabilan, što je još jedan od pokazatelja uspešnosti postavke arhitekture i verifikuje metodološki pristup.

⁶ Metodologija razvijena prema preporukama ECB a zasniva se na proceni uticaja rizika na CIA, i predlaganju mera iz kataloga na osnovu stepena procenjenog rizika

Predlog dokumenta koji predstavlja izlaz iz ovog koraka za primer centralne banke dat je u **prilogu 2, Sekcija 6.3.**

8.4. Operativna bezbednost – Ljudi

Ko su ljudi na operativnom nivou matrice bezbednosne arhitekture? To su svi oni koji su odgovorni za pravovremeno i tačno obavljanje bezbednosnih operacija, kako na upravljačkom tako i na pojedinačnom nivou. Takođe, ovde se definiše ko je odgovoran za dodelu korisničkih prava, za održavanje korisničkih računa, za upravljanje podrškom korisnicima. Podrška korisnicima mora da bude obezbeđena od početka do kraja kroz sve poslovne procese, odnosno za bezbednosne mehanizme koji pokrivaju te procese. Na isti način podrška mora biti obezbeđena i administratorima bezbednosnih rešenja i operatorima na sistemu. Ovakve podrške kod savremenih rešenja uglavnom su obezbeđene od proizvođača i to preko sertifikovanih osoba u vendara. Neretko, potrebno je omogućiti i udaljene veze, budući da su servisi decentralizovani i autorsovani. U svakom slučaju, moraju se identifikovati osobe za svaki deo životnog ciklusa bezbednosnog rešenja, kao i za reagovanje i eskalaciju incidenta.

Konkretno, to znači da je potrebno definisati organizacionu strukturu bezbednosti, uloge odgovornosti i sistem izveštavanja, programe podizanja svesti, treninge i plan razvijanja bezbednosne kulture, okvir upravljanja korisničkim pravima - dozvole i privilegije, role, IM, administraciju korisničkih naloga, personalne provere, kao i okvir podrške i organizacije help desk.

Centralna banka na ovaj segment arhitekture stavlja veliki naglasak. Posao je podeljen tako da su za izveštavanje i programe obuke zaduženi zaposleni koji se bave bezbednošću na nivou IT sektora, dok je administracija i podrška aplikacijama i korisnicima podeljena između administratora bezbednosti i administratora pojedinih infrastrukturnih oblasti. Vodi se računa da se administrativna ovlašćenja ne preklapaju (npr. administrator SIEM-a ne može biti administrator OS).

Predlog dokumenta koji predstavlja izlaz iz ovog koraka za primer centralne banke dat je u **prilogu 2, Sekcija 6.4.**

8.5. Operativna bezbednost – Lokacija

Prilikom odlučivanja gde će se postaviti bezbednosna rešenja, vodilo se računa o konfiguraciji mreže, potrebama posla i procenjenom riziku. Gde će se postaviti sistemi za operativno upravljanje bezbednosnim rešenjima zavisi i od lokacija tih rešenja, ali i od organizacionih kapaciteta organizacije. U ovom koraku definišu se sve specifičnosti upravljanja rešenjima bezbednosti na različitim lokacijama, upravljanje opremom, zgradama, platformama, mrežama i podmrežama. Upravljanje bezbednosnim okruženjem može biti centralizovano, ali to nije dobro

rešenje, osim ako je organizacija locirana tako. Ovaj korak zavisi takođe i od ljudskih kapaciteta kreiranih u prethodnom koraku i njihovog razmeštaja i organizacije. Lokacija upravljanja igra takođe veliku ulogu u planu kontinuiteta poslovanja, kao i u planovima za krizu i reagovanje na incidente.

U ovom koraku takođe se konkretno specificira upravljanje aplikativnom bezbednošću, bezbednošću na mreži, bezbednošću pojedinih platformi (Oracle, .NET itd.) bezbednošću internet sajta kao i bezbednošću pojedinačne opreme i svake radne stanice.

Centralna banka razvija upravljanje bezbednošću na svim platformama na kojima se odvijaju poslovne funkcije i servisi. Zahvaljujući dobro definisanim domenima i podeli posla u podršci infrastrukturi ovaj korak se lako realizuje na izlazima iz prethodnih, kako po horizontali tako i po vertikali SABSA matrice. Maksimalno se koriste ugrađene funkcionalnosti bezbednosti na pojedinim platformama, ali se povećava nivo znanja o njima (*Microsoft Security, Oracle Security, IBM Security...*) kako bi se podesile optimalne konfiguracije i obezbedila integracija infrastrukturnih rešenja različitih proizvođača. Prvi korak je obezbeđenje redovne nadgradnje i primene zakrpa, što nije jednostavno kad se uzme u obzir broj platformi i rešenja. Smanjenje kompleksnosti primenom integrisanih rešenja, povećavanje nivoa znanja i provere obezbeđuju potpunu pokrivenost uz minimalan uticaj na performanse.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka za primer centralne banke dat je u **prilogu 2, Sekcija 6.5.**

8.6. Operativna bezbednost – Vreme

Kada i u kom redosledu će se aktivirati i primeniti servisi za upravljanje bezbednošću? Ovde se definiše kalendar aktivnosti za praćenje i održavanje bezbednosnih rešenja. Kalendar mora uzimati u obzir i zahteve prihvaćene pri analizi rizika, kao i propise i zahteve relevantne industrije i podzakonska i interna akta. Važan aspekt u održavanju bezbednosnih mehanizama su i periodične provere. Periodične provere raspoređuju se tako da se bezbednosna rešenja koriste na najoptimalniji način i da se obezbedi puna pokrivenost poslovnih funkcija. Kao što se na svim sistemima vrše periodične provere upravljačkih mehanizama, isto je za bezbednosne mehanizme. Proveravaju se primene politika, implementacije mehanizama poput prava pristupa, rola, izvršavanje periodičnih provera bezbednosnih parametara, povezanost procesa i dokumentacije.

Izlaz iz ovog koraka je svojevrsni poslovni kalendar za upravljanje rasporedima vremena, kako poslovnih operacija tako i odgovarajućih bezbednosnih mehanizama. Definišu se i životni ciklusi aplikacija, posebno upravljanjem vremenima njihovog prekida i povlačenja iz produkcije. Potrebno je definisati sve vremenski zavisne procese, i upravljanje njima: životni ciklus korisničkog naloga i lozinke, životni ciklusi kriptografskih ključeva, vremenski zavisni konteksti upravljanja pristupom.

Upravo kao što je navedeno, i u slučaju centralne banke, a na osnovu prethodnih koraka, definišu se kalendari aktivnosti. Prethodni koraci u izgradnji arhitekture doveli su do jasnijeg identifikovanja svih kalendara i životnih ciklusa. Ovaj korak najviše od svih prethodnih doprinosi svojevrsnoj „higijeni“ arhitekture, jer eliminacijom zastarelih i neupotrebljivanih rešenja imamo efektivnije i efikasnije upravljanje životnim ciklusima bezbednosnih mehanizama u produkciji.

Predlog dokumenta koji predstavlja izlaz iz ovog koraka za primer centralne banke dat je u **prilogu 2, Sekcija 6.6.**

8.7. Operativna bezbednost kroz sve slojeve matrice

Već je pomenuto da poslednji sloj SABSA matrice zapravo i nije autonoman sloj na način kako su to ostali slojevi, i njegova funkcija je da objedini, prožima i na kraju podupre sve ostale slojeve konkretnim upravljačkim operacijama koje se izvode i od kojih se očekuju konkretni rezultati. Ta međuzavisnost se vidi u tome da je i prilikom samog definisanja koraka u opisivanju ovog sloja nemoguće dati definiciju koja će dati opis sloja samog po sebi – upravljanje ne znači ništa ako nije jasno čime se zapravo upravlja.

Kontekst arhitekture bezbednosti: Pogled poslovanja: Poslovni model rizika i Poslovni model procesa	Operativni sloj arhitekture bezbednosti: Pogled sa nivoa upravljanja infrastrukturom i objektima: Upravljanje operativnim rizikom Upravljanje bezbednosnim servisima
Koncept arhitekture bezbednosti: Pogled arhitekta: Ciljevi kontrola i Bezbednosne strategije i arhitektura	
Logička arhitektura bezbednosti: Pogled dizajnera: Bezbednosne politike i Bezbednosni servisi	
Fizička arhitektura bezbednosti: Pogled konstruktora: Bezbednosna pravila, prakse i procedure, Bezbednosni servisi	
Komponente arhitekture bezbednosti: Pogled prodavca: Bezbednosni standardi i Bezbednosni proizvodi i alati	

Slika 4: SABSA bezbednosna arhitektura

Posmatrajući interakciju operacija bezbednosti kroz sve ostale slojeve dolazi se do nečega što se može nazvati „**Arhitektura upravljanja bezbednosnim servisima**“, i što se zapravo interpretira operacijama bezbednosti definisanim nad svakim od prethodnih slojeva.

Tabela 1. prikazuje na konkretnim primerima kako se pojedine operativne aktivnosti izvršavaju na ostalim SABSA slojevima:

Sloj SABSA matrice	Operacije bezbednosti na sloju
Kontekstualna bezbednost	Rad na unapređenju pokretača poslovnih funkcija, aktivnosti na proveni rizika, upravljanje servisima, upravljanje relacijama, upravljanje snabdevanjem, upravljanje performansama
Koncept bezbednosti	Razvoj profila poslovnih atributa, razvijanje ciljeva upravljanja operativnim rizikom kroz aktivnosti procene, planiranje isporuke servisa, definisanje rola, odgovornosti i kulturoloških vrednosti u upravljanju servisima, upravljanje servisnim portfoliom, planiranje i održavanje servis kataloga i kriterijuma za performanse servisa, definisanje ciljeva (željenih nivoa) servisa.
Logički sloj bezbednosti	Upravljanje dobrima, upravljanje politikama, upravljanje pružanjem servisa, podrška korisnicima, upravljanje katalogom servisa, upravljanje evaluacijom servisa
Fizički sloj bezbednosti	Bezbednost i zaštita imovine, prikupljanje podataka iz procene operativnog rizika, upravljanje operacijama, podrška korisnicima na fizičkom nivou, zaštita servisnih resursa, prikupljanje podataka o servisnim performansama
Komponente bezbednosti	Zaštita alata, alati za upravljanje operativnim rizikom, puštanje novih alata u produkciju, upošljavanje osoblja, rukovanje alatima za upravljanje bezbednošću i alatima za monitoring servisa

Tabela 1. **Arhitektura upravljanja bezbednosnim servisima**

8.8. Pogled inspektora

Nakon što je šest etapa u razvoju bezbednosne arhitekture obrađeno kroz odgovarajuće "pogled", od poslovanja, preko arhitekta, dizajnera, graditelja, trgovca i serviser, važno je napomenuti da postoji još jedan pogled, a to je **pogled inspektora**. Naime, potrebno je obezbediti uverenje da je arhitektura kompletna, konzistentna, robustna i da odgovara nameni u svakom pogledu [1].

Ovo je zapravo proces auditinga, koga treba da sprovede sertifikovano osoblje. Zato je jasno zašto ga SABSA model ne prepoznaje kao poseban sloj – auditori treba utvrditi da li model podržava potrebe poslovanja. Postojanje dokumentovanih slojeva će im pomoći u tome, ali njihov inspektorski odnosno revizorski rad ne treba da zavisi od primenjenog modela. SABSA model pruža pomoć inspektorima u izvođenju struktuiranog ispitivanja, kao i da utvrdi da je bezbednost postavljena na sistematski i odgovarajući način.

Sa druge strane, uspostavljanje revizije i kontrole je definisano na konceptualnom sloju, dok su njihove aktivnosti definisane kroz operativni, odnosno upravljanje bezbednosnim servisima.

9. Vertikalni slojevi SABSA matrice

SABSA matrica sa svojih šest redova (nivo apstrakcije) i šest kolona (odgovori na pitanja) sačinjena je od 36 ćelija, gdje svaka predstavlja korak u radu, skup aktivnosti i dokumentacije, i gde se povezanoost ćelija sa susedima može posmatrati i po horizontali i po vertikali.

Prethodna analiza slojeva SABSA matrice rađena je po horizontali i to od slojeva više apstrakcije ka slojevima niže apstrakcije. Već je pomenuto da ovakav prikaz arhitekture nije slučajno nazvan matricom, budući da osim horizontalne sledljivosti postoji i vertikalna komponenta međuzavisnosti. Tako možemo posmatrati svaku od kolona, i pratiti kako se pojedine komponente razvijaju na nižim nivoima apstrakcije, i kako se zapravo odvijaju procesi u razvoju bezbednosne arhitekture.

1. Imovina – šta štitimo
2. Motivacija – zašto implementiramo bezbednost
3. Proces – kako će bezbednosni mehanizmi biti uklopljeni u poslovne procese
4. Ljudi – Koje su uloge i odgovornosti izvršilaca
5. Lokacija – Gde se i po kakvoj topologiji smeštaju komponente bezbednosti
6. Vreme – Kad i po kom rasporedu štitimo

Po svakoj od kolona prati se konkretizacija kategorija od definisanog konteksta pa do najnižeg nivoa apstrakcije a to su operacije u toj kategoriji.

10. Zaključak

Fizički sloj, sloj komponenti i operacije u SABSA matrici su oblast gde se stručnjaci IT bezbednosti uključuju sa konkretnim znanjima i iskustvima, i gde se već jasno vide konkretni obrisi arhitekture, a sa definisanjem operacija radi i njeno ukupno zaokruživanje.

U praksi, kad se radi implementacija bezbednosti po SABSA okviru, najteže je postaviti kontekstualni i logički sloj. Izazov za svaku organizaciju je da prikaže stvarno stanje, ali razlog zašto se to najčešće ne uspeva je što su katalozi servisa često nepotpuni ili ne postoje, a upravljanje konfiguracijama rasparčano i dokumentovano na više mesta, pa se teško vidi jasna slika o ukupnoj IT imovini.

Idealan je slučaj u kom se bezbednosna arhitektura postavlja pri samom kreiranju IT organizacije, ali to je moguće samo kod potpuno novih organizacija. Druga poželjna situacija je da postoji puna implementacija upravljanja rizikom, upravljanja procesima i upravljanja servisima, kao i potpuno dokumentovano upravljanje infrastrukturom.

Nažalost, takvi slučajevi se retko dešavaju u praksi, i najčešće je upravo implementacija bezbednosne arhitekture jedan od katalizatora koji treba da pomogne da se urede i prethodni

mehanizmi. Ovo je dobar primer na kom se može u praksi ispitati stvarna rešenost organizacije da napravi korak napred u razumevanju važnosti uloge IKT u celosti i bezbednosti IS kao krovnog mehanizma za otklanjanje rizika poslovanja.

Nadalje, kao što je rečeno na početku i prikazano na Slici 2, operativni sloj mora imati svoje obrise već već kod sagledavanja logičkog sloja. To se jasno videlo i u poglavlju 3 prvog dela rada, gde se fokus usmerava na informacije, radnike i domene, te se već nazire važnost operativnog rizika, upravljanja, kao i konkretnih bezbednosnih operacija.

Korišćenje SABSA metodologije nije samo upotrebljiv i koristan alat u uspostavljanju koncepta bezbednosne arhitekture organizacije, već analitičarima koji postavljaju pitanja stručnjacima za poslovne funkcije da nauče više o organizaciji, a samim nosiocima poslovnih funkcija da jasnije vide rizike i bolje sagledavaju stvarno stanje, što zajedno dodaje novu vrednost organizaciji u celini [7].

Na primeru koji je obrađivan tokom analize SABSA metodologije pokazala se tačnom pretpostavka da se bezbednosna arhitektura može postaviti u veliku organizaciju na način što će se to raditi iz sektora zaduženog za IKT, uz prethodno ispunjene uslove:

- Da su svi poslovi iz oblasti IKT vezani za poslovne funkcije objedinjeni pod nadležnost organizacionog dela koji se bavi IKT
- Da organizacioni deo koji se bavi IKT nadzire IKT imovinu, procese, da upravlja razvojem, infrastrukturom i operacijama u IKT
- Da postoji razumevanje i posvećenost najvišeg rukovodstva za značaj IKT u organizaciji
- Da postoji razumevanje i posvećenost najvišeg rukovodstva za važnost bezbednosti informacionog sistema
- Da se unutar organizacionog dela koji se bavi IKT shvati vlastita svrha, ne kao postojanje za sebe i radi sebe već radi omogućavanja poslovanja i obezbeđenja obavljanja poslovnih funkcija

Ovakva organizacija, odnosno njene poslovne funkcije potpuno su „vidljive“ iz sektora za IKT, postoji definisana saradnja sa nosiocima poslovnih funkcija koje se podržavaju pa je tako moguće i uraditi procenu rizika, a time postavku bezbednosne arhitekture.

Korišćeni primer odnosi se na organizaciju srednje veličine, sa povišenim stepenom bezbednosnih zahteva i donekle konzervativnim principima arhitekture. Međutim, koraci u SABSA metodologiji su dovoljno opšti da se može reći da je predloženi pristup realan i izvediv.

Opis skraćenica

IKT – Informaciono komunikacione tehnologije

IT - informacione tehnologije (korišteno za naziv org. dela, stara terminologija)

ROI – Return Of Investment

SD – Service Desk

IM – Identity Manager

AD – Active Directory

CM – Configuration Manager

IRM – Information Risk Management

CA – Criticality Assessment

ORM – Operational Risk Management

ACL – Access Control List

RBAC – Role Based Access Control

ECB – European Central Bank

BIS – Bank for International Settlement

SLA – Service Level Agreement

OLA – Operational Level Agreement

NOC – Network Operational Center

SOC – Security Operational Center

CERT – Telo ili organizacija koja prikuplja i obrađuje podatke o bezbednosnim incidentima i brine o informisanju zajednice, preporukama i širenju bezbednosne kulture

AV – Anti Virus

DLP – Data Leakage Protection

Literatura:

- [1] Sherwood, J., Clark, A. & Lynas, D. (2005.), *Enterprise Security Architecture – A Business-Driven Approach*, CRC Press , Taylor&Francis Group, NewYork
- [2] Krag Brotby, (2009) *Information Security Governance, A practical Development and Implementation Approach*, – Appendix A: SABSA Business Attributes and Metrics
- [3] Petković, R., Babić, S. *Analiza poslovanja i informaciona bezbednost* <http://www.infotech.org.rs/blog/wp-content/uploads/radovi2013/072.pdf> pristupano 24.10.2014.
- [4] Grubor, G., (2012), *Projektovanje menadžment sistema zaštite informacija*, Univerzitet Singidunum, Beograd.
- [5] Milosavljević, M.i Mišković, V.(2011), *Elektronska Trgovina*, Univerzitet Singidunum, Beograd.
- [6] Battersby, M., (2013), *SABSA, A Brief Introduction*, White Paper, Capgemini 2013.
- [7] <http://www.batimes.com/articles/addressing-information-security-in-business-analysis-with-sabsa.html> pristupano 25.05.2015.

Prilog 1.**SABSA Matrica razvoja bezbednosne arhitekture**

	Dobro (ŠTA)	Motivacija (ZAŠTO)	Proces (KAKO)	Ljudi (KO)	Lokacija (GDE)	Vreme (KAD)
Kontekstualno	Poslovne funkcije	Poslovni model rizika	Poslovni model procesa	Organizacija poslovnih funkcija i međusobne relacije	Poslovna geografija	Vremenske zavisnosti poslovnih funkcija
Konceptualno	Poslovni atributi i profili	Ciljevi koje želimo postići kontrolama	Bezbednosne strategije i slojevitost arhitekture	Model personala sda stanovišta bezbednosti Uloge i ovlašćenja	Bezbednosni domeni	Životni ciklusi i rokovi u kontekstu bezbednosti
Logički	Poslovni informacioni model	Bezbednosne politike	Bezbednosni servisi	Šema zaposlenih i profili privilegija	Definicije bezbednosnih domena i pridruženi entiteti	Životni ciklusi bezbednosnih procesa
Fizički	Poslovni model podataka	Bezbednosna pravila, prakse i procedure	Bezbednosni mehanizmi	Korisnici, aplikacije i korisnički interfejsi	Platforme i mrežna infrastruktura	Puštanje u rad kontrolnih struktura
Komponente	Detaljna struktura podataka	Bezbednosni standardi	Bezbednosni proizvodi i alati	Identiteti, funkcije, akcije i ACL.	Procesi, čvorovi, adrese i protokoli	Koraci i vremena u implementaciji bezb.
Operativno	Obezbeđenje operativnog kontinuiteta	Oupravljanje operativnim rizikom	Upravljanje i podrška bezbednosnim servisima	Upravljanje i podrška aplikacijama i korisnicima	Bezbednost sajtova i platformi	Kalendar (redosled) bezbednosnih operacije

Prilog 2.

Poslovna jedinica	1. KONTEKST ARHITEKTURE BEZBEDNOSTI	Datum:
IT NBS		Verzija:
1.1. Poslovne funkcije		
Delatnost	Obezbeđenje IKT servisa u cilju podrške ispunjavanjima poslovnih ciljeva NBS, i to kroz: održavanje infrastrukture, razvoja i održavanja aplikacija, podršku korisnicima i brigu o bezbednosti informacija.	
Cilj	Visoka raspoloživost i pouzdanost IKT	
Opis ciljeva i zadataka	Integracija IKT funkcija, optimizacija procesa, održavanje tehnološke savremenosti, održavanje i unapređenje nivoa znanja i kompetencije zaposlenih, donošenje politika bezbednosti, podizanje svesti o bezbednosti i primena mera i kontrola....	
Sredstva za postizanje cilja: - Broj i struktura zaposlenih - HW inform. imovina - SW inform. imovina	Navedeni repozitorijumi se nalaze inicijalno u Osnovnim Sredstvima (OS) i podacima Ljudskih resursa (LJR), a za potrebe IT integrisani u Active Directory (AD), Identity Manager (IM) i Service Desk aplikaciju (SD). Kad se radi o hardverskoj i OS arhitekturi, konfiguracije se održavaju kroz Configuration Manager (CM) Podaci o obrazovanju su u LJR, kao i neke od dodatnih obuka (samo one koje je finansirala NBS), dok su broj zaposlenih, potrebne kompetencije i radni zadaci pojedinog radnog mesta opisane u Organizaciji i Sistematizaciji radnih mesta. Aplikativni portfolio je takođe integrisan u SD.	
Lokacije poslovanja	6 lokacija u Beogradu, Novi sad, Užice, Kragujevac, Niš (prilog je šema)	
Poslovni procesi i korisnici	Link na dokument "Upravljanje procesima". Dokument je izrađen prema COBIT5 preporukama. Opširnije u 1.3.	
Okvir za implementaciju bezb. rešenja	ISO 27002 kao osnov za Politike bezbednosti informacija u NBS	
Predloženi tip rešenja	Kombinovano rešenje: zaštita na mreži, standardi aplikativne bezbednosti, podizanje svesti zaposlenih	
Karakteristike rešenja	"Defence in Depth" pristup, postavljanje više slojeva zaštite	
Posebni uslovi	Čvrsto opredeljenje rukovodstva da se elementi bezbednosti implementiraju planski i da se postavlja sveobuhvatna zaštita, da se pojedini elementi integrišu, te da se pažnja posveti punoj implementaciji procesa upravljanja rizikom. Klasifikacija informacija je bitan uslov.	
Veze sa ostalim dokumentima	Politike bezbednosti informacija u NBS, Šifarnik OS, Organizacija i sistematizacija radnih mesta (realno, ovde bi išle oznake dokumenata iz sistema označavanja)	
Napomena	Analiza je utvrdila da su u SD samo preneti podaci o OS, te da se ne vode pojedinačne konfiguracije, pa bi bilo dobro da se i to ažurira sa podacima iz CM. Nadalje, podaci o IT kompetencijama ne postoje, i bilo bi dobro da se i u IT sektoru vodi evidencija o stvarnim znanjima i veštinama pojedinih zaposlenih. CM ne obuhvata Unix (Linux) servere i Ubuntu radne stanice. Ovaj deo je u fazi unapređenja, jer nova verzija CM to podržava Klasifikacija informacija još nije završena.	

Prilog 2.

1.2. Poslovni model rizika	
Dokumenta upravljanja rizikom	Metodologija IRM, CA, Katalog bezbednosti, Metodologija ORM, Lista rizika
Metodologija	Metodologija IRM u ECB, Metodologija ORM u ECB
Veze sa ostalim dokumentima	Praćenje aplikativnog projekta, Stanje infrastrukture, Procedure za upravljanje izmenama, Procedure za upravljanje incidentima
Napomena	Budući da je opseg dokumenta IT NBS, ne postoji krovna procena rizičnosti pojedinih poslovnih procesa u NBS, već se polazi od procene kritičnosti aplikacija koje podržavaju pojedine poslovne procese
1.3. Poslovni model procesa	
Model procesa sa procenom kritičnosti	Link na dokument "Upravljanje procesima". Dokument je izrađen prema COBIT5 preporukama.
Metodologija	Usvojena je COBIT 5 metodologija za opisivanje procesa
Podaci i informacije proistekli iz procesa i njihova klasifikacija	Model podataka i informacija se nalazi u opisima šema baza i strukturama datoteka. U toku je proces utvrđivanja stepena tajnosti i klasifikacija
Veze sa ostalim dokumentima	
Napomena	
1.4. Organizacija poslovnih funkcija i odnosi (ljudski resurs)	
Interna struktura zaposlenih	Sistematizacija radnih mesta
Regulativa koja definiše odnos zaposlenih i organizacije	Pravilnik o radu, Pravilnik o poslovnom ponašanju, Ugovor o radu
Eksterni resursi	Ugovori o obavljanju povremenih poslova, Ugovori o održavanju, Ugovori o poslovno-tehničkoj saradnji
Posebni uslovi	Regulativa koja se odnosi na sprečavanje sukoba interesa
Praćenje ovlašćenja po poslovnim i IT funkcijama	Identity Manager, Active Directory
Veze sa ostalim dokumentima	
Napomena	
1.5. Poslovna geografija	
Geografske lokacije	Adrese objekata BG 1-5, NS, NI, UE, KG
Čvorišta IKT	Šema mrežne infrastrukture
Vrste udaljenog pristupa	LAN, WAN, VPN, Internet Optički link, iznajmljene linije, ISDN,
Distribuirana rešenja	CM – upravljanje konfiguracijom Distribucija aplikacija: klasične web aplikacije, Oracle Forms aplikacije sa web

Prilog 2.

	filozofijom(plugin na klijentu), ClickOnce distribucija , klasična klijent-server distribucija.
Zakonski okviri, standardi i ograničenja	
Procena interoperabilnosti bezb. rešenja	Infrastruktura mreže predviđa da su bezbednosna rešenja svuda jednako efikasna i uklopljena u ostala rešenja sa što manje negativnog uticaja Sprovode se obuke i programi podizanja svesti Postoji povratna informacija o upoznatosti zaposlenih sa sadržajem politika
Veze sa ostalim dokumentima	
Napomena	Ne postoji politika za mobilne uređaje niti BYOD politika, niti podležu bezbednosnim kontrolama, osim laptop računara koji su vlasništvo NBS. U toku je analiza.
1.6. Vremenske zavisnosti poslovnih funkcija	
Radno vreme	Pored utvrđenog radnog vremena NBS, IT sektor posluje i prema posebnim odlukama o radnom vremenu koje podrazumevaju dežurstva. Pokriveno je vreme 07-22 h.
Specifične poslovne funkcije	Specifični poslovi su vezani za poslove trezora, Platni sistem, platne kartice Internet portal je 24/7 , ali je procenjeno da rizik od nedostupnosti u neradno vreme nije velik
Zahtevi za raspoloživost	Većim delom je ti 7,30-17,00 , s tim što se zbog poslovnih funkcija obezbeđuju dežurstva i pokriva vreme 07-22 Zahtev Centra za platne kartice je 0-24 , ali još se rešava
Sinhronizacija	Time Server
Novi servisi/procesi	Network Operational Center (NOC) i Security Operational Center (SOC) koji se planiraju će doneti i nove zahteve za posebnim radnim vremenom i dežurstvima
Veze sa ostalim dokumentima	
Napomena	

Prilog 2.

Poslovna jedinica	2. KONCEPT ARHITEKTURE BEZBEDNOSTI	Datum:
IT NBS		Verzija:
2.1. Poslovni atributi		
Taksonomija poslovnih atributa	Veza na Taksonomija poslovnih atributa za NBS, podela na obavezne i opcione attribute	
Strategija analize rizika poslovanja	Za sada kroz IRM i CA	
Standardizacija poslovnih zahteva	Dokumentacija kojom se reguliše praćenje projekta, upravljanje promenama, i kontrola kvaliteta	
Profili atributa (ako je urađeno profilisanje)	Ideja je da se u budućnosti profilišu poslovne funkcije. Unutar IT sektora, administratorska funkcija bi mogla biti nosilac posebnog profila	
Veze s ostalim dokumentima		
Napomena	Inženjering poslovnih zahteva je važan korak i treba da bude implementiran kroz procedure, makar to uzima dodatno vreme.	
2.2. Ciljevi koje želimo postići bezbednosnim kontrolama		
Opšti ciljevi	Poverljivost, integritet, raspoloživost	
Rizici po profilima	(nakon profilisanja proceniti rizik za profil)	
Rizici nedostizanja ciljeva		
Veze s ostalim dokumentima		
Napomena		
2.3. Bezbednosne strategije i slojevitost arhitekture		
Fizička bezbednost	Kontrola pristupa, ID kartice,restriktivne zone	
Bezbednost mreže	Navesti uređaje i tehnike	
Mehanizmi pristupa	Politika kontrole pristupa	
PKI i enkripcija	Navesti rešenja i gde se koriste	
Aplikativna bezbednost	“Opšti okvir upravljanja aplikativnom bezbednošću u NBS”	
Mehanizmi prema kategoriji zahteva	Specifične poslovne celine: Platni sistem, Platne kartice, ZIN ...	
Veze sa ostalim dokumentima		
Napomena		
2.4. Model personala sa stanovišta bezbednosti		
Način regulisanja uloga i ovlašćenja	-Sistematizacija radnih mesta -Metodologija izrade procedura i instrukcija kao deo sistema kvaliteta predviđa definisanje uloga i odgovornosti za svaki korak procesa	
Upravljačka funkcija	Svaka politika, okvir, procedura, uputstvo mora biti odobrena od rukovodstva	
Korisnička funkcija	Odgovornost u skladu sa Politikom	
Treća lica	Ugovorne obaveze, poslovanje u dobroj nameri, (Ugovorima je definisan i nivo	

Prilog 2.

	poverenja)
Ugovori i sporazumi	
Vlasništvo	Vlasništvo nad aplikacijama, podacima, lične odgovornosti (procesi, oprema)
Koncept poverenja	Ugovori različitog sadržaja, kategorizacija partnera (gold, silver, bronze, npr.)
Podaci o aplikacijama	Za svaku aplikaciju iz portfolija mora postojati ko je odgovoran za njeno funkcionisanje, te ko je vlasnik podataka, imovine, ko je zastupnik ukoliko se radi o trećem licu, kakvi su uslovi održavanja i slično.
Veze sa ostalim dokumentima	
Napomena	
2.5. Bezbednosni domeni	
Pokrivenost kontrolama	Obezbeđeno redovnim kontrolama i revizijama
Fizički domeni	Infrastruktura mreže (kabliranje), fizičke lokacije opreme i zaposlenih
Logički domeni	Mrežna infrastruktura na višim slojevima, AD, IM, mejl server, distribucija aplikacija ...
Specifični segmenti	Platni sistem, Platne kartice, ZIN,
Nepokriveni segmenti	Mobilni uređaji za sada
Veze sa ostalim dokumentima	
Napomena	
2.6. Životni ciklusi i rokovi	
Prihvaćeni standardi i metodologije	ITIL, COBIT, ISO 20000 ...
Praćenje projekta (bezbednost)	Ovde upisati načine na koje se kontrolišu bezbednosne pretpostavke kroz životni ciklus proizvoda ili servisa koji je predmet projekta (ili razvoja, ako se izrađuje kao modul).
Upravljanje promenama	Ovde postoje dva aspekta, jedan je kontrola bezbednosnih mehanizama u slučaju bilo koje promene (npr ako se radi o aplikativnom rešenju, ponekad je potrebno uraditi ponovnu procenu kritičnosti i reviziju kontrole), a drugi aspekt je kad je sampo bezbednosno rešenje predmet promene.
Penzionisanje starih rešenja	Naveći mehanizam kako se prati penzionisanje aplikativnih odnosno infrastrukturnih rešenja, i u skladu sa tim i penzionisanje relevantnih bezbednosnih rešenja ili delova. Takođe, pojedina bezbednosna rešenja bivaju penzionisana kad se zamene novim ,ili se promeni koncept zaštite.
Posebni rizici	Ukoliko iz procene rizika proizlazi da je određena oprema zastarela, pa stoga podložna riziku (npr. radne stanice sa Win95) , ili neku ranjivu infrastrukturu
Veze sa ostalim dokumentima	
Napomena	

Prilog 2.

Poslovna jedinica	3. LOGIČKA POSTAVKA ARHITEKTURE BEZBEDNOSTI	Datum:
IT NBS		Verzija:
3.1. Poslovni informacioni model		
Poslovne informacije prema modelu procesa	Šema procesa kao krovni dokument – deo razrade procesa po slojevima, a zatim šeme baza podataka, projektna dokumentacija, konkretna IRM dokumentacija	
Načini čuvanja	Regulisano pravilnikom i procedurama bekapa	
Načini razmene	Standardni protokoli, procedure za razmenu	
Poverljivost	Mehanizmi zaštite	
Integritet	Mehanizmi zaštite	
Dostupnost	Mehanizmi zaštite	
Veze sa ostalim dokumentima		
Napomena		
3.2. Bezbednosne politike		
Opšta politika	Politika upravljanja bezbednošću	
Posebne politike	Politika bezbednog pristupa, Politika korišćenja interneta, Politika upravljanje incidentima	
Primenjeni standardi	ISO 27002	
Upravljanje rizikom	Metodologija IRM, metodologija ORM	
Veze sa ostalim dokumentima		
Napomena		
3.3. Bezbednosni servisi		
Servis poverljivosti	Potvrditi postojanje servisa	
Servis integriteta		
Servis autentifikacije		
Servis kontrole pristupa		
Servis neporecivosti		
Servis dostupnosti		
Veze sa ostalim dokumentima		
Napomena	Ovde navesti nepostojanje određenih servisa, postojanje rizika,specifičnosti i sl.	
3.4. Šema zaposlenih i profili privilegija		
Broj i struktura zaposlenih po nivoima privilegija	Ovde navesti vrste radnih mesta, broj izvršilaca i privilegije koje ta radna mesta nose	
Procedura eskalacije i degradacije privilegija	Sinhronizacija kadrovske evidencije i IM, odobrenje rukovodstva	
Procedura ukidanja	Sinhronizacija kadrovske evidencije i IM	

Prilog 2.

prava i privilegija	
Dodela prava	Odobrenje rukovodstva
Specijalna prava	
Zaposleni na bezbednosti i njihova prava	
Načini čuvanja root lozinki	Root lozinke se ne koriste u praksi, i u principu se drže zaključane u sefu
Veze sa ostalim dokumentima	
Napomena	
3.5. Definicije bezbednosnih domena i pridruženi entiteti	
Bezbednosni domeni na AD	U okviru AD definišu se poddomeni i grupe, zavisno od lokacije i specifičnih poslova (navesti)
Bezbednosni domeni na IM	IM realizuje promene u organizaciji konsultujući promene u evidenciji ljudskih resursa
Bezbednosni domeni na mrežnoj opremi	Primer: Grupe sa specifičnim pravima u oblasti filtriranja izlaska na web Kategorizacija VPN korisnika (navesti) Kategorizacija korisnika IP telefonije (navesti)
Bezbednosni domeni na mejl serverima	
Pravila o preklapanju domena	
Specijalni domeni	Vip korisnici, platni sistem....
Veze sa ostalim dokumentima	
Napomena	
3.6. Životni ciklusi bezbednosnih procesa	
Vremenski zavisna bezbednosna rešenja	(pobrojati rešenja koja ne rade kontinuirano, i koja se uključuju po potrebi) Pobrojati rešenja kojima ističe održavanje u određenom periodu Upravljanje sertifikatima.
Rešenja planirana za zamenu	Pobrojati servise koji su planirani za povlačenje ili postoje preporuke za to (ovde su i mrežni servisi, npr, ali i pojedini algoritmi, npr kriptografski, servisi kontrole pristupa itd)
Rešenja planirana za implementaciju	Npr. prijava putem kartica koje će sadržavati sertifikat
Bezbednosna rešenja zavisna od poslovnih procesa	Npr. kontrole koje sprovodi AD odnose se na zaposlene (dakle proces zapošljavanje – rad (sa izmenama)-napuštanje) Administrativni moduli pojedinih IKT rešenja za sprovođenje praćenja upravljanja ljudskim resursima (ovde pobrojati triplete: poslovni proces – IKT rešenje – zaštita , i analizirati dobijena odstupanja)

Prilog 2.

Kontrola postojanja poslovnog procesa koji se štiti	- Periodične provere pristupa resursima - Predlaganje resursa i servisa za penzoinisanje - Pronalaženje softvera koji nije redovno “zakrpljen” - Pronalaženje softvera koji niko više ne koristi, a dostupan je

Prilog 2.

Poslovna jedinica	4. FIZIČKA POSTAVKA ARHITEKTURE BEZBEDNOSTI	Datum:
IT NBS		Verzija:
4.1. Poslovni model podataka		
Model - poslovni	- po šemama BP - po aplikacijama	
Model infrastruktura	- podaci infrastrukture, AD, IM – načini organizacije podataka , prikupljanje, čuvanje, bekap - podaci servis desk aplikacije	
Autsorsing	Modeli podataka u autsorsovanim rešenjima i kupljenim aplikacijama i servisima	
Bezbednost	Modeli podataka bezbednosti (korisnička imena, lozinke, sertifikati, ključevi...)	
Veze sa ostalim dokumentima	Ovde se navode i poslovni zahtevi, kao i podaci sektora ljudskih resursa	
Napomena		
4.2. Bezbednosna pravila, prakse i procedure		
Pravila	Naveći subpolitike kao što je upravljanje lozinkama, upravljanje elektronskom poštom, pristup Internetu, fizički pristup resursima, ulazak u salu...)	
Procedure	Nabrojati procedure koje definišu procese zasnovane na bezbednosnim politikama	
Uputstva	Nabrojati korisnička uputstva koja regulišu postupanje po konkretnim situacijama (npr. Uputstvo za prijavu bezbednosnog incidenta)	
Prakse	Procena rizika, puštanje u rad, arhitektura posistema, izbor platformi	
Nenapisana dokumentacija	Prepoznata dokumenta koja nedostaju	
Veze sa ostalim dokumentima		
Napomena		
4.3. Bezbednosni mehanizmi		
Zaštita na perimetru i fizički mehanizmi	Lista mehanizama	
Proceduralna zaštita		
Upravljačka zaštita		
Veze sa ostalim dokumentima		
Napomena	Ovde navesti nepostojanje određenih servisa, postojanje rizika, specifičnosti i sl.	
4.4. Korisnici, aplikacije i korisnički interfejsi		
Lista aplikacija	Lista aplikacija sa korisnicima i interfejsima i šta se odnosi na bezbednosne mehanizme na interfejsu (npr. aplikacija vođenja evidencije o prisustvu na poslu je osnovna za radno mesto evidentičara, ali određene promene zahtevaju	

Prilog 2.

	odobravanje rukovodioca, i njegov pristup aplikaciji je kroz drugačiji interfejs, i vidi različit skup podataka)
Ap-Int-Kor	Uređene trojke (aplikacija, interfejs, korisnik)
Standardi	Interni standardi za interfejse i podela po tipovima, kategorijama...
API	Liste korištenih API i njihove karakteristike
Analiza	Analiza interfejsa, uočene nepravilnosti, predlozi za smanjenje kompleksnosti
Veze sa ostalim dokumentima	
Napomena	
4.5. Platforme i mrežna infrastruktura	
Topologija mreže	Dijagram
Mrežna oprema	Taksonomija i opis mrežne opreme, spisak
Platforme	
Veze i propusnost	
Planovi za konfiguracije	
Veze sa ostalim dokumentima	
Napomena	
4.6. Puštanje u rad kontrolnih struktura	
Model	Model životnog ciklusa
Vremena	Vreme rada po mehanizmima (posebno za specifične mehanizme)
Periodične provere	Vremenski intervali ugrađenih i upravljanih provera
Veze sa ostalim dokumentima	
Napomena	

Prilog 2.

Poslovna jedinica	5. KOMPONENTE ARHITEKTURE BEZBEDNOSTI	Datum:
IT NBS		Verzija:
5.1. Detaljna struktura podataka		
BP Detaljno	Detaljne strukture podataka po bazama, sa opisima polja i sintaksnim pravilima	
Ostale evidencije	Ručno rađeni spiskovi i evidencije bitni za poslovanje	
Poslovne aplikacije	Aplikativni portfolio	
Hardver	Hardverske komponente	
Procesori	Specifikacija procesorskih jedinica	
Memorijske jedinice	Specifikacija memorijskih jedinica	
Rečnici	Rečnik podataka i metapodataka	
Veze sa ostalim dokumentima	Detaljni poslovni zahtev	
Napomena		
5.2. Bezbednosni standardi		
Lista	Lista primenjenih i konsultovanih standarda i u kojim oblastima (npr ISO27000, NIST za bezbednost, ISO20000 servisi, ISO 31000 upravljanje rizikom, ITIL, COBIT i sl.)	
Veze sa ostalim dokumentima		
Napomena		
5.3. Bezbednosni proizvodi i alati		
Administracija korisnika	Kako je regulisano, ko radi, tehničke specifikacije ...	
Praćenje logova		
Bekap		
Monitoring		
Veze sa ostalim dokumentima		
Napomena	Ovde navesti nepostojanje određenih servisa, postojanje rizika, specifičnosti i sl.	
5.4. Identiteti, funkcije, akcije i ACL		
Imenovanje		
Role		
Opisi poslova		
Parovi radno mesto – akcija na sistemu		

Prilog 2.

Privilegije	
Iznimke	
Veze sa ostalim dokumentima	
Napomena	
5.5. Procesi, čvorovi, adrese i protokoli	
Skica bezbednosne arhitekture	Dijagram, šematski prikaz po čvorovima u mreži
Aplikacije	
Protokoli	
Adrese i portovi	
Veze sa ostalim dokumentima	
Napomena	
5.6. Koraci i vremena u implementaciji bezbednosti	
Dijagram toka	Koraci implementacije bezbednosti u vremenskim okvirima
Specifična vremena	
Kritična vremena	
Veze sa ostalim dokumentima	Pravilnik o utvrđivanju radnog vremena (sa odredbama koje se odnose na iznimke i posebno radno vreme)
Napomena	

Prilog 2.

Poslovna jedinica	6. OPERATIVNA IZVEDBA ARHITEKTURE BEZBEDNOSTI	Datum:
IT NBS		Verzija:
6.1. Obezbeđenje operativnog kontinuiteta		
Plan implementacije	Planovi za svako bezbednosno rešenje ili komponentu	
Izvedeno stanje	Ne samo za implementirane komponente, nego i veće promene, npr. posle svakog pečovanja piše se izvedeno stanje	
Poslovni zahtevi		
Klasifikacija informacija		
BC plan		
Opšti upravljački okviri		
Veze sa ostalim dokumentima	BC plan	
Napomena		
6.2. Upravljanje operativnim rizikom		
Procenjeni rizik	Dokumentacija o upravljanju operativnim rizikom	
Revizija kartica rizika		
Revizija politika		
Periodične provere		
Testiranje na ranjivosti i penetracioni testovi		
Veze sa ostalim dokumentima	Pregled ranjivosti i pretnji	
Napomena		
6.3. Upravljanje i podrška bezbednosnim servisima		
Upravljanje bezbednošću IS	Metodologija za upravljanje informatičkim rizikom , podaci o proceni i primenjenim kontrolama po projektima	
Upravljanje incidentima		
Oporavak od pada		
Upravljanje promenama		
IDS/IPS		
SIEM		
Operativne procedure	Određivanje i implementacija pravila, PKI infrastruktura, održavanje pristupnih lista, administriranje SIEM	
Veze sa ostalim dokumentima		
Napomena		

Prilog 2.

6.4. Upravljanje i podrška aplikacijama i korisnicima	
Organizaciona struktura	Uloge i odgovornosti zaposlenih u bezbednosti, linija obaveštavanja i izveštavanja
Programi obuke	Plan i programi obuke podizanja svesti, treninzi, testovi
Privilegovan pristup	Opisi pristupnih metoda i primenjene kontrole, pravila za administratorske naloge, logovanje, rukovanje sa datotekama lozinki
Veze sa ostalim dokumentima	
Napomena	
6.5. Bezbednost sajtova i platformi	
Poslovne oblasti	
Bezbednosni domeni	Upravljanje bezbednošću po domenima
Bezbednost aplikacija	Testiranje, kvalitet softvera, OWASP, WAF
Bezbednost mreže	
Bezbednost internet sajta i portala	
Bezbednost radnih stanica	
Ostala oprema	
Veze sa ostalim dokumentima	
Napomena	
6.6. Kalendar (redosled) bezbednosnih operacija	
Poslovni kalendar	Trajanje licenci, implementacije rešenja, testovi (<i>proof of concept</i>)
Bezbednosne operacije	Definisanje rasporeda, bezbednosnih kontrola i provera
Životni ciklus aplikacija	
Upravljanje vremenski zavisnim mehanizmima	Životni ciklusi korisničkih imena Životni ciklusi lozinki Životni ciklusi mejlboksa Životni ciklusi kriptografskih ključeva
Redosledi operacija	Bezbednosne operacije koje imaju utvrđene redoslede izvršavanja
Veze sa ostalim dokumentima	
Napomena	

Prilog 3 . Primer profila sa atributima

