

UPRAVLJANJE RIZIKOM METODOM OCTAVE-S

ppuk. sc Gorazd Zavodnik, dipl. inž., Vojna akademija Vojske Srbije,
gorazd_z@lycos.com

Rezime: U kreiranju programa zaštite jedan od ključnih koraka je procena i analiza rizika. To je polazna tačka za uvođenje i održavanje sistema zaštite i smanjenja rizika na najmanji moguć nivo. Jedna od metoda za upravljanje rizikom je OCTAVE (za srednje i velike organizacije) odnosno OCTAVE-S (za manje organizacije). Ove metode sprovode zaposleni u organizacijama, a usmereni su na identifikaciju pretnji za kritične IKT objekte organizacije i donošenje strategijskih odluka.

Ključne reči: Rizik, ranjivost, pretnje, analiza, politika zaštite

RISK MANAGEMENT USING OCTAVE-S METHOD

Abstract: In creating a protection program one of key steps is risk evaluation and analysis. This is a starting point for implementing and maintaining a protection system and reducing risk to the lowest possible level. One of risk management methods is OCTAVE (for medium and large organisations) or OCTAVE-S (for small organisations). These methods are conducted by employees in the organisations and their scopes are identification of threats to organisations' critical ICT assets and making of strategical decisions.

Keywords: Risk, vulnerability, threats, analysis, protection policy

UVOD

Procesi upravljanja rizikom i analize rizika kritične su komponente programa zaštite jer identifikuju najveći mogući broj ranjivosti sistema, koji se uopšte može otkriti. U praksi se termin **upravljanje rizikom** često koristi jedinstveno i obuhvata upravljanje i analizu rizika. Procena rizika jedan je od ključnih koraka u kreiranju programa zaštite, bez kojeg organizacija ne može znati šta treba štititi, koji nivo zaštite treba implementirati i po kojoj ceni i šta organizacija smatra da je odgovarajuća redukcija rizika na prihvatljivom nivou.

Glavna aktivnost u **upravljanju rizikom** je identifikacija i specifikacija bezbednosnih mera i metoda za implementaciju radi postizanja optimalnog nivoa zaštite, ili redukcije procenjenog rizika do prihvatljivog nivoa. Zavisno od namene, u procesu upravljanja rizikom bezbednosne mere i metode sistema zaštite mogu se podeliti i svrstati po efikasnosti u nekoliko grupa. Neke mere je lakše i jeftinije uvesti u ranoj fazi životnog ciklusa sistema.

U idealnom slučaju, uprava organizacije treba da odredi nivo prihvatljivog i neprihvatljivog rizika, koji je specifičan za svaku organizaciju. Koliki je nivo rizika prihvatljiv, zavisi od misije, internih standarda, vrednosti objekta, kulture organizacije i volje uprave da prihvati rizik.

Danas je svako ranjiv. Postoji tehnička ranjivost - računarske infrastrukture i aplikacije (izgled, primena, konfiguracija) i organizacijska ranjivost (resursi, sistem obezbeđenja, korisnici, saradnici, klijenti, snabdevači, ...). Ranjivosti i incidenti mogu dovesti do gubitka ili uništavanja poverljivih informacija, uvid u lične podatka klijenata, povrede regulative, gubitak kontakata i slično, što iziskuje potrebu da se organizacije i podaci zaštite. Metoda OCTAVE je samo jedna od raspoloživih metoda za procenu i upravljanje rizikom.

1. UPRAVLJANJE RIZIKOM

Upravljanje rizikom u informaciono-komunikacionim tehnologijama (IKT) je sveukupan proces uspostavljanja i održavanja sistema zaštite IKT objekata. Analizom se rizik identifikuje i procenjuje, tako da se opravdaju troškovi uvođenja i održavanja sistema zaštite. Cilj analize rizika je obezbeđivanje rentabilne i savremene zaštite koja odgovara realnim pretnjama kao i da se izbegnu neracionalno skupe i kontraproduktivne zaštitne mere.

Termin „upravljanje rizikom“ se često koristi jedinstveno i obuhvata upravljanje i analizu rizika. Te kritične komponente programa zaštite identifikuju najveći mogući broj ranjivosti sistema. Bez procene organizacija ne može da zna, šta, kako i po kojim ceni treba štititi i šta je redukcija rizika na prihvatljivi nivo. U idealnom slučaju najviša upravna struktura organizacije treba da odredi nivo prihvatljivog i neprihvatljivog rizika.

Misija sistema zaštite je zaštita IKT objekata kroz izbor, instalaciju i održavanje sistema zaštite na prihvatljivom nivou rizika od pretnji koje ga ugrožavaju. Kontrolne funkcije zaštitnih mera i metoda se biraju tako da se dostigne izbalansirana i komplementarna zaštita. U takvom sistemu su manje efikasne mere i metode zaštite komplementirane efikasnijim merama i metodama, a tehničke mere zaštite praćene su netehničkim merama.

Metodologija analize, procene i proračuna rizika

Generalno, kod svih metoda u prvoj fazi potrebno je sačiniti spisak digitalnih objekata IKT sistema¹, njihove vrednosti i osetljivosti za organizaciju. Sledi procena scenarija mogućih izvora pretnji od strane potencijalnih napadača i prirodnih nepogoda. Procenjuje se koja bi oprema mogla privući napadače i na koji način. Zatim projektni tim vrši simulaciju probijanja svog sistema zaštite i procenjuje potencijalni scenario realizovanih napada i faktora rizika. Procena faktora rizika može biti valjana za neko vreme i ako se temeljito uradi, ali se scenario pretnji brzo menja pa se i procena mora sukcesivno ažurirati.

Procena vrednosti objekata zasniva se na generalno prihvatljivim merama kvaliteta digitalnih objekata: poverljivosti, raspoloživosti i integriteta. Identifikaciju i procenu vrednosti ili osetljivosti imovine vrši se unutar granica bezbednosnog rizika u IKT sistemu, koje moraju biti korektno uspostavljene i ništa što može uticati na bezbednost sistema ne sme ostati izvan tih granica. Potrebno je odrediti težinske faktora za svaki objekat pojedinačno, a skala težinskih faktora je stvar izbora svake organizacije.

Procena ranjivosti odnosi se na mogućnosti gubitaka ili šteta u sistemu. Rangiranje tačaka ranjivosti vrši se prema proceni potencijalne štete koja može nastati zloupotrebom te ranjivosti od strane nekog agenta pretnje. Težinske faktore treba procenjivati i računati za svaku tačku ranjivosti, a određuju se u odnosu na vidljivost, korisnost, trajnost, iskoristivost i zaštićenost objekata IKT sistema. Ranjivost postoji u hardveru, softveru, poslovnim procesima i ljudima i često je teško proceniti ranjivost objekta IKT sistema pre incidenta.

Procena pretnji se odnosi na klasifikaciju izvora pretnji i mogu se grupisati na razne načine. Pretnje mogu na različite načine uticati na IKT sisteme. One mogu biti **slučajne** i **namerne**. Uticaj može biti **primaran** (neovlašćen pristup podacima) i **sekundaran** (prirodne nepogode).

Procena uticaja odnosi se na procenu verovatnoće da će određene, najčešće kombinovane pretnje iskoristiti date ranjivosti sistema, kao i na intenzitet tog iskorišćenja.

2. METOD OCTAVE

Metod evaluacije operativno kritičnih pretnji, informacionih ili digitalnih objekata IKT sistema i ranjivosti sistema OCTAVE (*Operationally Critical, Threat, Asset and Vulnerability Evaluation*) omogućava organizacijama da identifikuju faktore rizika za najznačajnije objekte IKT sistema i da izgrade plan mera zaštite da se eliminišu, smanje ili ublaže ti faktori rizika.

Osnovni koncept metoda OCTAVE zasniva se na sledećim činjenicama:

- nije moguće redukovati ili otkloniti sav rizik za IKT sistem,
- finansijska sredstva i drugi resursi za zaštitu uvek su ograničeni,
- ne mogu se sprečiti svi odlučni i sofisticirani napadi na sistem,
- kompjuterski incidenti se moraju prepoznati i neutralisati, a sistem se mora oporaviti,
- potrebno je na najbolji mogući način iskoristiti raspoložive resurse da se obezbedi preživljavanje minimalno neophodnih radnih funkcija IKT sistema i organizacije.

Za razliku od tipičnih metoda rizika koji su orijentisani na tehnološki rizik i fokusirani na taktička pitanja, OCTAVE je usmeren na rizik poslovanja organizacije i

¹ Digitalni ili informacioni objekti obuhvataju sve fizičke i logičke objekte IKT sistema koji procesiraju, kladište ili prenose digitalne podatke.

fokusiran na strategijske aktivnosti koje se odnose na praksu zaštite. To je fleksibilna evaluacija koja se može prilagoditi za većinu organizacija, a sprovodi je tim sastavljen od zaposlenih u organizaciji.

Metod OCTAVE obuhvata tri faze evaluacije:

- Faza 1: Identifikacija i izrada profila pretnji;
- Faza 2: Analiza ranjivosti;
- Faza 3: Planiranje i razvoj strategije i plana zaštite.

Bitni elementi ili zahtevi metoda OCTAVE su ugrađeni u skup kriterijuma i u vezi sa ovim razvijena su dva metoda:

- metod OCTAVE (za srednje i velike organizacije) i
- metod **OCTAVE –S** (za male organizacije).

U složenom procesu **proaktivne zaštite** IKT sistema, aktivnosti OCTAVE kreiraju jedan opšti pogled organizacije na tekući bezbednosni rizik za informacione objekte, obezbeđujući direktan i brz uvid u svako vreme, ili referentnu osnovu, koja se može koristiti za usmeravanje aktivnosti za smanjenje rizika i poboljšanje prakse zaštite. U toku realizacije metoda OCTAVE analitički tim izvršava tri sledeće ključne aktivnosti:

- identifikuje bezbednosni rizik informacionih objekata organizacije,
- analizira faktore rizika i određuje prioritete rizika i
- planira i **izrađuje** strategiju smanjenja rizika i plan zaštite kritičnih objekata organizacije za smanjenje rizika i poboljšanje prakse zaštite.

Da bi poboljšala sistem zaštite kritičnih objekata, organizacija mora identifikovati faktore rizika za te objekte, analizirati ih i proceniti, a zatim planirati strategiju i mere zaštite u procesu reinženjeringa sistema zaštite, izvršavanjem sledećih aktivnosti:

- planiranje i implementacija strategije zaštite i smanjenja faktora rizika,
- monitoring (nadzor) dinamike sprovođenja i efektivnosti realizacije akcionih planova i
- kontrola varijacija u izvršavanju plana i preduzimanje korektivnih aktivnosti.

Evaluacija bezbednosnog rizika informacionih objekata je deo aktivnosti organizacije u procesu upravljanja rizikom. Metod OCTAVE je evaluacioni proces koji ima svoj početak i kraj. OCTAVE aktivnosti izvršavaju procese identifikacije stanja sistema zaštite, analize faktora rizika i planiranja strategije i mera zaštite za smanjenje rizika na prihvatljivi nivo. Proces upravljanja rizikom definisan je i zatvoren izvršavanjem cikličnih aktivnosti: *planiranja, implementacije, kontrole i korekcije* sistema zaštite.

3. METOD OCTAVE-S

OCTAVE-S je varijanta pristupa primerenija ograničenjima i jedinstvenim pokazateljima tipičnim za male organizacije (do 100 zaposlenih). OCTAVE-S predvodi mali interdisciplinarni tim (3 do 5 ljudi) sačinjen od zaposlenih, koji prikupljaju i analiziraju informacije, koji predlažu strategiju i planove zaštite, zasnovane na jedinstvenim bezbednosnim rizicima. Za uspešno sprovođenje, OCTAVE-S tim treba da dobro poznaje poslovanje organizacije i procese zaštite. Iako se razlikuje od metoda OCTAVE, daje iste tipove rezultata, uključujući strategiju zaštite za IKT sistem celokupne organizacije.

Pre pokušaja korišćenja OCTAVE-S potrebno je shvatiti sledeća dva jedinstvena aspekta metode:

- Mali interdisciplinarni tim od 3 do 5 ljudi predvodi OCTAVE-S. Kolektivno, članovi tima za analizu treba da poseduju širok uvid u poslovanje i bezbednosnu politiku organizacije, potreban za sprovođenje svih aktivnosti;

- OCTAVE-S uključuje ograničeno istraživanje IKT infrastrukture u fazi 2. Pošto male organizacije često iznajmljuju IKT servise i funkcije, pa u tom slučaju tim ispituje procese za bezbedno konfigurisanje i održavanje IKT infrastrukture.

3.1. Proces OCTAVE-S

OCTAVE-S je samovodeća evaluacija bezbednosnih pretnji. Zahteva analitički tim za ispitivanje bezbednosnih pretnji i stvaranje politike zaštite i planova za umanjenje rizika. Implementacijom rezultata OCTAVE-S organizacija nastoji da bolje zaštiti IKT resurse i poboljša celokupno stanje bezbednosti.

3.1.1. Faza 1: Izrada profila pretnji

Faza 1 je evaluacija stanja organizacije. Tim definiše uticaj evaluacionih kriterijuma koji će kasnije biti korišćeni za procenu rizika, identifikuje bitne elemente i procenjuje tekuću praksu zaštite organizacije. Tim sam završava sve zadatke, tražeći dodatne informacije kada je neophodno. Nakon toga bira 3 do 5 kritičnih elemenata za dublju analizu zasnovanu na njihovoj važnosti za organizaciju i definiše bezbednosne zahteve i profil pretnji za svaki kritični element.

Ova faza obuhvata procese S1 (Identifikacija informacija organizacije) i S2 (Kreiranje profila pretnji).

3.1.2. Faza 2: Identifikacija infrastrukturnih ranjivosti

Kroz ovu fazu analitički tim sprovodi analizu IKT strukture organizacije, fokusirajući se na stepen zaštite koju sprovode održavaoci infrastrukture. Analizira se kako zaposleni koriste IKT infrastrukturu za pristup kritičnim elementima, definisanjem ključnih klasa komponenti, kao i ko je odgovoran za konfigurisanje i održavanje tih komponenti i ispituje se do koje mere odgovorni sprovode bezbednosne mere vezane za procedure i procese. Ova faza obuhvata proces S3 (Ispitivanje IKT infrastrukture u odnosu na kritične elemente).

3.1.3. Faza 3: Razvoj bezbednosne strategije i planova

Kroz fazu 3 tim identifikuje kritične pretnje i odlučuje šta će preduzeti. Na osnovu analize prikupljenih informacija tim formira strategiju zaštite organizacije i planove ublažavanja pretnji kritičnim elementima.

Ova faza obuhvata procese S4 (Identifikacija i analiza pretnji) i S5 (Razvoj strategije zaštite i planova za ublažavanje).

3.2. Izlazi OCTAVE-S

Upravljanje pretnjama po informacionu bezbednost zahteva ravnotežu između reaktivnih i proaktivnih aktivnosti. Kroz procenu putem OCTAVE-S analitički tim posmatra bezbednost iz raznih uglova, nastojeći da uravnoteže preporuke sa potrebama organizacije. Glavni izlazni rezultati ove faze su: strategija zaštite

organizacije, planovi smanjenja pretnji i spisak aktivnosti. Pored toga korisni su i: listing bitnih IKT elemenata koji podržavaju ciljeve poslovanja organizacije, izveštaj o ispunjavanju dobre prakse zaštite i profil pretnji za svaki element.

3.2.1. Područje primene

OCTAVE-S je razvijana i začeta u malim organizacijama (20 do 80 zaposlenih), koje su imale neke zajedničke karakteristike: relativno nerazgranata organizaciona struktura, zaposleni na raznim organizacionim nivoima su obično sarađivali i često su izvršavali više zadataka u raznim celinama organizacije. Takve organizacije su, dakle, mogle okupiti tim od tri do pet članova, koji je uključivao:

- zaposlene sa različitih nivoa organizacije, uključujući rukovodstvo i
- koji su imali široko znanje o poslovanju i bezbednosnim procesima organizacije.

Organizacija, bez obzira na veličinu, koje je u stanju da formira odgovarajući tim, potencijalno je dobar kandidat za sprovođenje OCTAVE-S. Na primer, organizacija sa jednostavnom strukturom i sa oko 200 zaposlenih, koji su u toku godina rada prošli kroz većinu odeljenja, dobar je kandidat za sprovođenje metoda OCTAVE-S. Sa druge strane, organizacija sa oko 80 zaposlenih koji su raštrkani na više mesta i sa izuzetno usmerenom organizacijskom strukturom (zaposleni u raznim odeljenjima ne sarađuju mnogo međusobno), po svojoj prilici nije kandidat za OCTAVE-S.

3.2.2. Mogućnost korišćenja OCTAVE-S

Sledeći skup pitanja treba da pomogne prilikom određivanja da li je metod OCTAVE-S primenljiv u organizaciji:

- Da li je organizacija mala? Da li i ma ravnu ili jednostavnu hijerarhijsku strukturu?
- Može li se naći grupa do 3 do 5 ljudi za analitički tim koji imaju široko i duboko razumevanje poslovanja kompanije i koji poseduju većinu od sledećih veština: umeće rešavanja problema, analitičko umeće, umeće timskog rada, bar jedan član sa rukovodećim veštinama i mogućnost da provede nekoliko dana radeći na metodu.
- Da li razumete sve ili većinu funkcija informatičke tehnologije?
- Da li je IKT infrastruktura relativno jednostavna i dobro shvaćena od strane bar jednog zaposlenog u organizaciji?
- Da li ima ograničenja u poznavanju alata za procenu ranjivosti u kontekstu analize IKT objekata ili nema mogućnosti preuzimanja ekspertize od spoljnih saradnika radi interpretacije rezultata?
- Da li ima prednost visokostrukturirana metoda nasuprot otvorenoj metodi koju je lakše prilagoditi?

Ako su svi odgovori "Da", onda je OCTAVE-S pravi izbor. U slučaju većine odgovora "Da" OCTAVE-S može biti dobar izbor, ali uz oprez. Iako OCTAVE-S može biti funkcionalan izvan tih granica, rezultati nisu zagarantovani.

3.3. Pripreme za izvođenje

Aktivnosti na pripremi OCTAVE-S su važne jer određuju stepen uspešnosti procene. Kroz pripremu se određuje način sprovođenja OCTAVE-S. Bitni faktori za uspeh su: podrška rukovodstva, izbor analitičkog tima i određivanje cilja procene.

3.3.1. Podrška rukovodstva (aktivnost S0.1)

Podrška rukovodstva je najkritičniji faktor za uspeh procene pretnji. Uspešna procena traži značajno angažovanje zaposlenih. Ukoliko uprava podržava proces, zaposleni će aktivnije učestvovati, u suprotnom, volja će brzo nestati.

3.3.2. Izbor tima (aktivnost S0.2)

Analitički tim je centralna tačka sprovođenja OCTAVE-S. Odgovoran je za konačni uspeh procene, a članovi treba da poseduju dovoljne veštine, iskustva i ekspertizu za vođenje procene. U opštem slučaju za formiranje tima potrebno je pridržavati se sledećih principa:

- analitički tim se sastoji od tri do pet članova,
- može se formirati tim za podršku ukoliko neki proces zahteva specifične veštine ili znanja,
- u timu se obično nalaze zaposleni iz raznih delova organizacije (i rukovodioci),
- tim mora imati širok uvid u poslovanje i IKT infrastrukturu,
- perspektive poslovanja i IKT infrastrukture raspoložive su timu u najvećoj mogućoj meri.

Tim pomaže u određivanju obima procene i odgovoran je za identifikaciju ključnih stvari i analizu informacija. Podrškom može rukovoditi jedan od članova tima, a može se angažovati i dodatno lice ako specifičnosti to zahtevaju.

OCTAVE-S počiva na iskustvu i ekspertizi članova tima i za efektivnu procenu članovi treba da imaju uvid u:

- način korišćenja sistema i informacija u podržavanju poslovnih procesa,
- politiku i procese u organizaciji,
- procese koji se koriste za konfigurisanje i održavanje IKT infrastrukture.

Članovi tima moraju imati dobre radne odnose, čime otvorenije dele brigu o bezbednosti organizacije, a potrebne veštine su:

- sposobnost vođenja sastanaka grupe,
- dobre veštine komunikacije,
- dobre analitičke veštine,
- poznavanje poslovnog okruženja organizacije i poznavanje IKT okruženja i
- način korišćenja IKT tehnologije.

Od zaposlenih, koji imaju uvid u način korišćenja sistema i informacija za podršku poslovanja, kao i uvid u politike i procese organizacije, biraju se do tri člana tima. Drugi deo tima čine zaposleni u IKT infrastrukturi.

Nakon izbora članova tima, bar jedan član (u idealnom slučaju, svi) treba da se upozna sa OCTAVE-S, što zavisi od mogućnosti organizacije. Izabrani član (članovi) mogu učestvovati u formalnoj obuci ili mogu samostalno izučavati potrebnu literaturu.

Ukoliko se krene bez obuke, svi članovi tima moraju pročitati odgovarajuću literaturu i prodiskutovati metod međusobno. Nakon toga treba sprovesti ograničeni pilot projekat birajući element koji je kritičan za organizaciju, čime tim stiče razumevanje procesa procene i rada sa informacijama prikupljenim kroz tok procene. Potrebno je prodiskutovati, šta je bilo teško, a šta lako i potrebno je izvršiti pripreme i planiranje proširene procene.

Ukoliko rukovodstvo podrži proširenu procenu, treba skrenuti pažnju na to da će, bez formalne obuke a uz samostalno učenje, proces procene trajati duže nego što je planirano.

3.3.3. Postavljanje obima procene (aktivnost S0.3)

Mnoge male organizacije mogu biti u potpunosti procenjene sa OCTAVE-S, a moguće je i fokusirati procenu na izabrane delove organizacije. Postavljanje odgovarajućeg obima za evaluaciju smanjuje njen obim čineći je lakšom za planiranje i izvođenje aktivnosti. Takođe je dozvoljeno određivanje prioriternih delova organizacije čime će najveće pretnje ili najbitnija područja biti ispitana prva ili češće.

Kada bira područja za procenu, analitički tim po pravilu sarađuje sa rukovodstvom organizacije. Pri tome se razmatra sledeće:

- izbor celina koje odražavaju glavne operativne ili poslovne funkcije kao i važne funkcije za podršku organizacije,
- poželjno je izabrati najmanje četiri celine, od kojih jedna mora biti odeljenje za informatiku (ili ljudi koji poznaju IKT infrastrukturu, ako takvo odeljenje ne postoji),
- ukoliko organizacija većinu ili kompletno upravljanje IKT poverava vanjskim saradnicima, treba izabrati ljude koji tesno sarađuju sa njima, ili njihove predstavnike,
- ako je odeljenje za informatiku raspršeno ili podeljeno na više grupa, bira se celo područje,
- procena vremena angažovanja osoblja i uticaj na redovne poslove,
- razmatranje područja koja zahtevaju elektronske informacije za izvršavanje svojih funkcija.

Za izbor celina za procenu razmatra se i:

- koje celine su najkritičnije za postizanje cilja,
- koje celine mogu svojim nefunkcionisanjem ugroziti funkcionisanje organizacije,
- u kojim celinama su informacije ili sistemi najpodložniji pretnjama.

Ukoliko je tim već formiran, a neki članovi nemaju dovoljan uvid u izabrane celine, neophodno je promeniti sastav tima.

3.3.4. Planiranje izvođenja OCTAVE-S (aktivnost S0.4)

OCTAVE-S se mora planirati kao i bilo koji drugi projekat u organizaciji. Tim mora delovati zajednički kroz svaku aktivnost, tako da svaki član treba da odvoji dovoljno vremena za završetak svake aktivnosti. Svaki proces ima sledeće sekcije:

- ulazni kriterijumi,
- zahtevane veštine,
- učesnici (određuju se za svaki proces),
- procena vremena (za svaku aktivnost),
- izlazni kriterijumi.

Kroz planiranje izrađuje se i redosled procene. Potrebno je:

- odlučiti, kada će tim sprovoditi svaki OCTAVE-S proces,
- odlučiti, da li neki proces, ili aktivnost zahteva dodatno osoblje,
- odrediti potrebno vreme za pripremu za svaki proces,
- pretpostaviti potrebno vreme za završetak (za obe vrste timova).

U toku izrade plana treba razmotriti koliko članovi tima poznaju OCTAVE-S, informatičku bezbednost i upravljanje pretnjama. Zavisno od iskustva planiraju se potrebna vremena za realizaciju pojedinih procesa..

3.3.5. Priprema za izvođenje svakog OCTAVE-S procesa (aktivnost S0.5)

Tim treba da bude spreman za svaku aktivnost. To uključuje spremnost za sprovođenje svakog procesa i obezbeđenje potrebne podrške.

Pre početka bilo kojeg procesa tim mora obezbediti sve ulazne kriterijume. Takođe članovi tima treba da razumeju svoje uloge i način na koji treba da sprovedu zahtevane aktivnosti. I pridruženi članovi treba da razumeju svoje uloge u procesu u kojem učestvuju. Na kraju, članovi se moraju složiti o načinu donošenja odluka koji je razumljiv svima, čime se obezbeđuje nedvosmisleni rad tima prilikom rešavanja problema i donošenja odluka.

Koraci za obezbeđenje podrške su direktni i lako razumljivi, ali mogu da predstavljaju i veliku prepreku u toku procene. Podrška uključuje planiranje "radionica", obezbeđenje potrebne opreme za sastanke i koordinaciju rasporeda članova tima. Za koordinaciju podrške treba da bude zadužen jedan član tima.

3.3.6. Prilagođavanje OCTAVE-S

Analitički tim određuje u kolikoj meri će izvršiti prilagođavanje OCTAVE-S u toku planiranja. Potrebno je razmišljati o jedinstvenim potrebama organizacije i koje aspekte metode treba prilagoditi da bi se uskladile sa tim potrebama. Postoje dva opcionalna zadatka u OCTAVE-S za koje analitički tim mora sprovesti prilagođavanje: *verovatnoća* i *potvrda rezultata procene*.

Verovatnoća je procena mogućnosti da se događaj (pretnja) desi. Određivanje verovatnoće za svaku pretnju se smatra opcionim. Kod pretnji informacionoj bezbednosti verovatnoća je kompleksnija i nepreciznija promenljiva u odnosu na ostale domene upravljanja pretnjama, pošto se faktori pretnji neprestano menjaju. Treba je koristiti pažljivo zbog visoke subjektivnosti i nedostatka objektivnih podataka.

OCTAVE-S uključuje kvalitativnu verziju verovatnoće. Zasniva se na mogućnostima analitičkog tima da pretpostavi pokretanje i istoriju raznih tipova napada i pretnji. Ne treba zaboraviti da proces donošenja odluka počiva primarno na uticaju pretnji. Procena uticaja pretnji na date ranjivosti sistema koristi se za odlučivanje o ublažavanju ili prihvatanju rizika.

Potvrda rezultata procene zavisi od sastava tima i njegovih ovlašćenja. Zavisno od toga rukovodstvo može tražiti potvrdu rezultata pre preduzimanja bilo kakve formalne akcije za implementaciju tih rezultata. To se dešava u slučaju da rukovodilac, koji je član tima, nema ovlašćenja za odobravanje planova za ublažavanje rizika. U tom slučaju potrebno je organizovati sastanak sa rukovodstvom nakon procesa S5.

Ostale aktivnosti za prilagođavanje su diskreciono pravo tima, ali prilagođavanje nije uvek jednostavno. Mogu se prilagođavati:

- katalog praksi,
- opšti profil pretnji,
- kategorije objekata za procenu,
- kategorije bezbednosnih zahteva,
- kriterijumi za procenu uticaja, i
- radni listovi.

4. ZAKLJUČAK

Metod OCTAVE je strateški pristup zasnovan na pretnjama i planiranju tehnika za zaštitu. Radi se o samonavodećem metodu, što znači da zaposleni treba da prihvate odgovornost za uspostavljanje bezbednosne strategije organizacije. OCTAVE metod podiže nivo poznavanja prakse i procesa zaštite u cilju sagledavanja trenutnog stanja bezbednosti. Za razliku od tipičnog pristupa zasnovanog na tehnologiji, koji se više bave tehnološkim pretnjama i taktičkim odlukama, metod OCTAVE je težišno usmeren na organizacijske pretnje i donošenje strateških odluka.

5. LITERATURA

1. Dorofee A., Alberts C., Woody C. (2004), Information Assurance in Small Organizations
2. Grubor mr Gojko, dipl. inž. el. (2005), Upravljanje rizikom (predavanje na FPI)
3. Alberts C., Dorofee A., Allen J. (2001), OCTAVE Catalog of Practices, V2 (www.cert.org)
4. Alberts C., Dorofee A., Stevens J., Woody C. (2005), OCTAVE®-S Implementation Guide, Version 1.0 (www.cert.org)