

ANALIZA I PROCENA RIZIKA

Analiza i procena rizika određuje verovatnoću nastajanja rizika, analizu međuzavisnosti rizičnih događaja, kvantifikacija uticaja pojedinih događaja ili njihove kombinacije na sistem. To je procedura koja se koristi za procenu verovatnoće pretnji i potencijalnog gubitka koji može rezultirati iz osetljivosti sistema. Krajnji cilj analize rizika je da pomogne u izboru **troškovno prihvatljivih mera za zaštite** koje reduciraju rizik na prihvatljiv nivo.

Za obavljanje analize rizika na raspolaganju su brojne metode i tehnike koje se međusobno razlikuju po prirodi, širini i dubini obuhvata. O njihovoj primeni na procenjivanje problema zaštite treba odlučivati na osnovu njihove mogućnosti da obezbede razumne i dokumentovane odgovore na fundamentalna pitanja vezana za dizajniranje i implementaciju sistema zaštite u konkretnom IS. Veličinu mogućeg uticaja identifikacija rizika moguće je odrediti preko:

- Kvantitativne analize podrazumevaju analizu u kojoj se rizik izražava i procenjuje (izračunava) numeričkim kvantitativnim parametrima, kao i uticaj rizika na ciljeve projekta i verovatnoća da do tih rizičnih događaja dođe.

- Kvalitativne procene se vrše na osnovu faktora fleksibilnost sistema i verovatnoća za promenama u IS. Primer: nizak, umeren ili visok nivo rizika. Upravljanje rizikom se može definisati kao skup upravljačkih metoda i tehnika kojima se minimiziraju gubici i dovode u sklad troškovi kojima se smanjuje verovatnoća ostvarenja gubitka sa troškovima koji bi nastali od rizičnog događaja. Zapravo, sprovodi se neka vrsta cost/benefit analize.

Ključni faktori rizika su:

1. Sam rizični događaj, pojava ili aktivnost koji mogu da prouzrokuju štete ili neželjene posledice po informacioni sistem.
2. Verovatnoća pojavljivanja rizičnog događaja.
3. Veličina uloga, odnosno, veličina gubitka koji može da nastane ako se ostvari rizični događaj.

Za procenu rizika koristi se jednačina:

$r = f \cdot g$, gde je: r - rizik, f - frekvencija (verovatnoća) nastajanja pretnje, g - jednokratni gubitak (veličina moguće štete). Ovo su ključni elementi analize rizika. Treba za svaku identifikovanu pretnju u odnosu na posmatrani objekat utvrditi *verovatnoću nastajanja* i *veličinu štete* (izraženu numeričkim ili verbalnim kvalifikatorom) koju pretnja može izazvati, imajući pri tome u vidu da je jedini factor nesigurnosti vremenski okvir u kojem će se neka pretnja realizovati, a ne i da li će se realizovati.

Kod utvrđivanja verovatnoće nastajanja identifikovanih pretnji mora se polaziti od konkretnog ambijenta i realnih uslova, jer, na primer, verovatnoća pojave nekih prirodnih katastrofa može biti vrlo velika u nekim geografskim područjima, dok je u drugim ta pretnja beznačajna; izloženost terorističkim akcijama karakteristična je za kontraverzna područja i za informacione sisteme posebne namene. Osnovu za formiranje skupa efikasnih mera zaštite može da obezbediti samo sistematična analiza rizika. U tu svrhu često se kao polazna tačka koristi **matrica analize rizika rizika**.

Svaki element matrice (A1 - E3) označava jednu kategoriju rizika koju predstavlja određena kategorija pretnji za određeni objekat, pri čemu se i objekti i pretnje mogu dalje razvijati do željenog nivoa detaljnosti. Za uspešno razrešavanje problema analize rizika kojima su izloženi objekti zaštite, kao pogodno sredstvo sa praktičnog stanovišta preporučuje se korišćenje tabela, koje pružaju sistematičan i dokumentovan pristup.