https://www.pexels.com/photo/photo-of-person-holding-mobile-phone-3183153/

OSNOVNI POJMOVI UPRAVLJANJA RIZIKOM I KONTINUITETOM POSLOVANJA

PRIJAVITE SVAKI INCIDENT
NA NAŠEM PORTALU

SRB-CERT

OSNOVNI POJMOVI UPRAVLJANJA RIZIKOM I KONTINUITETOM POSLOVANJA

Bez upotrebe informacionih tehnologija poslovne organizacije[1] ne mogu zamisliti svoje poslovanje. Proces digitalizacije je unapredio poslovanje, doneo brojne benefite, ali se paralelno sa razvojem novih tehnologija povećalaizloženost rizicima i pretnjama, što može imati uticaj na imovinu, zaposlene, informacije, druge organizacije, kao i na samo poslovanje.

Pretnje po informacioni sistem uključuju prekide pod uticajem okoline, ljudske greške, hardverske greške, sajber napade koji su često dobro organizovani i veoma sofisticirani, a posledice mogu biti katastrofalne po organizacije.

Učestalost sajber napada je sve veća i prisutnija u državnim institucijama, finansijskim institucijama, udruženjima, ali i u malim i srednjim preduzećima, a koji za cilj imaju narušavanje ugleda i reputacije, krađu podataka ili identiteta, prekid poslovanja, finansijske prevare, novčane iznude i dr. Činjenica je da je sajber napade sve teže detektovati i adekvatno i pravovremeno reagovati, odnosno nije moguće u potpunosti se zaštititi, stoga je veoma važno definisati planove i akcije kojima se precizira šta treba uraditi kada se sajber napad dogodi. Unapred definisani rizici kao i načini postupanja mogu biti dobar način umanjenja posledica prouzrokovanih sajber napadima.

Poslovne organizacije izložene su različitim vrstama rizika koji mogu ozbiljno ugroziti njihovo poslovanje. U cilju obezbeđivanja poslovanja u slučaju neželjenog događaja neophodno je preventivno planiranje i preduzimanje koraka radi umanjenja posledica, omogućavanja nastavka rada i oporavka od neplaniranih prekida poslovnih funkcija.

Upravljanje kontinuitetom poslovanja (*Business Continuity Management* - **BCM**) je pristup celokupnom poslovanju koji se sastoji od politika, procedura, smernica i sa njima povezanih resursa, organizacionih uloga, odgovornosti, ovlašćenja, kao i planiranja aktivnosti koje omogućavaju funkcionisanje u slučaju nepredviđenih okolnosti.

BCM obuhvata **Plan kontinuiteta poslovanja** (*Business Continuity Plan* - **BCP**) koji opisuje pristup proceni prekida, planiranja oporavka od prekida, i stalnog praćenja oporavka. Dobar plan podrazumeva dobro urađenu identifikaciju, analizu i evaluaciju rizika, definisane ključne procese, adekvatno implementirano rešenje za oporavak sistema, plan aktivnosti i dodeljenih odgovornosti.

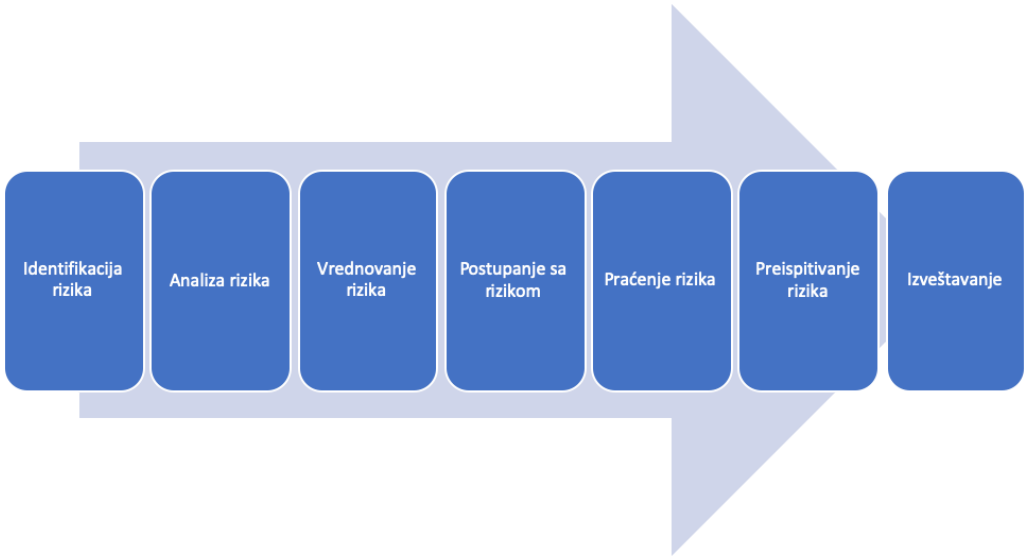
Primerena procena rizika identifikuje pretnje i ranjivosti kojima je izložena organizacija, procenjujući verovatnoću da će se neki događaj dogoditi i njegovu potencijalnu posledicu (Slika 1). Na temelju toga se može odrediti i proceniti stvarna izloženost riziku i učinkovito planirati ulaganja kako bi se postigao očekivani nivo bezbednosti IKT sistema.

[1] Poslovna organizacija obuhvata, ali nije ograničena na preduzetnike, kompaniju, korporaciju, firmu, preduzeće, organ vlasti, partnerstvo, dobrotvornu organizaciju ili instituciju, ili njihov deo ili kombinaciju, bez obzira na to da li su objedinjeni ili ne i da li su javnog ili privatnog karaktera.

Slika 1 - Nastanak bezbednosnih incidenata

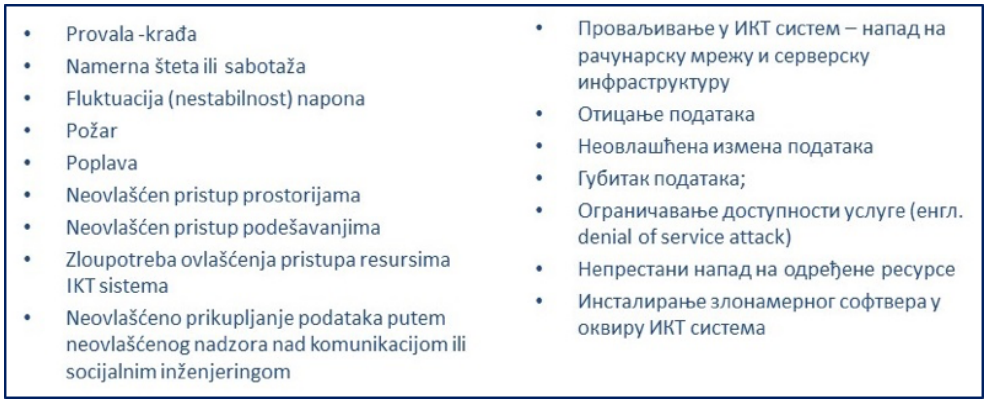
Rizik je kombinacija posledica nekog događaja (uključujući i promene u okolnostima) i povezane verovatnoće nastanka. U kontekstu informacione bezbednosti, rizici po bezbednost informacija mogu se izraziti kao efekat nesigurnosti na ciljeve bezbednosti informacija.

Upravljanje rizikom je proces koji obuhvata sistematsku primenu politika menadžmenta, procedura i prakse na aktivnosti komuniciranja, konsultovanja, uspostavljanja konteksta i identifikovanja, analiziranja, vrednovanja, postupanja, praćenja, preispitivanja i izveštavanja o svim rizicima koji mogu uticati na dostizanje strateških i finansijskih ciljeva organizacije (Slika 2).

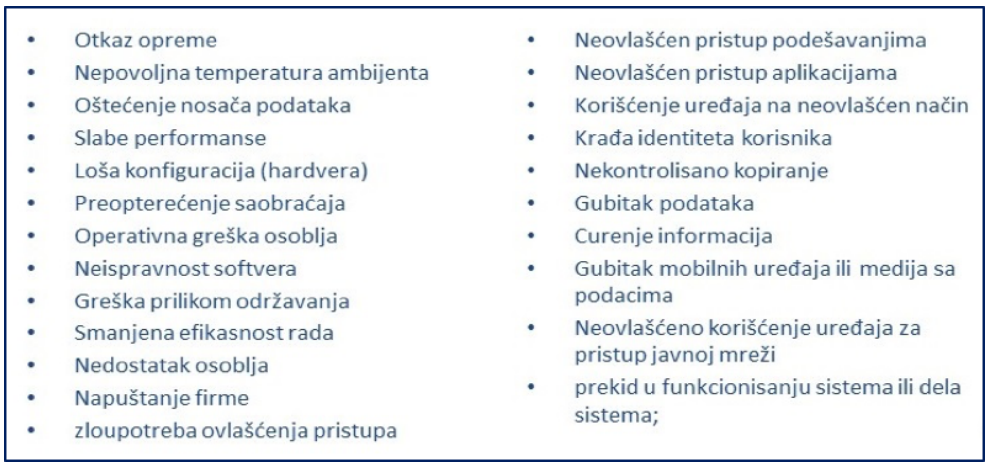


Slika 2 – Proces upravljanja rizikom

Identifikacija rizika podrazumeva pronalaženje, prepoznavanje i opisivanje rizika koji mogu pomoći ili sprečiti organizaciju da postigne svoje ciljeve. Oblici spoljnih pretnji koji se mogu javiti prilikom identifikacije rizika prikazani su na Slici 3, dok su oblici unutrašnjih pretnji prikazani na Slici 4.



Slika 3 – Oblici spoljnih pretnji



Slika 4 – Oblici unutrašnjih pretnji

Analiza rizika je proces razumevanja prirode rizika i utvrđivanja nivoa rizika.

Vrednovanje rizika zahteva ocenjivanje rizika i metodu postupanja sa rizikom, koja može obuhvatiti procenu troškova i koristi, zakonske obaveze, brigu o zainteresovanim stranama i drugim ulaznim elementima. Ovim postupkom je potrebno kvantifikovati i odrediti prioritete rizika prema kriterijumima za prihvatanje, odnosno neprihvatanje rizika.

Moguće opcije za **postupanje sa rizikom** obuhvataju sledeće odluke:

- Primenjivanje odgovarajućih mera da bi se rizici otklonili ili smanjili;
- Promena verovatnoće nastanka rizika;
- Promena posledica;
- Znalački i objektivno prihvatanje rizika, obezbeđujući da oni jasno zadovolje politiku organizacije i kriterijume za prihvatanje rizika;
- Izbegavanje rizika ne dopuštajući mere koje bi dovele do pojave rizika, odnosno da se ne počinje ili ne nastavlja sa aktivnošću koja dovodi do rizika
- Deljenje rizika sa drugom stranom ili stranama, na primer osiguravajućim kućama.

Tokom celokupnog procesa upravljanja rizikom treba imati u vidu da postupanje sa rizikom može stvoriti nove rizike ili modifikovati postojeće.

Svrha **nadgledanja i praćenja rizika** je poboljšanje kvaliteta i efikasnosti primene rezultata procesa za postupanja sa rizikom, snimanjem rezultata i pružanjem povratnih informacija.

Celokupan proces upravljanja rizikom i rezultate procesa je potrebno dokumentovati i vršiti **izveštavanje** pomoću odgovarajućih mehanizama. Na taj način se pružaju informacije koje su potrebne za donošenje odluka, poboljšanje aktivnosti za upravljanje rizikom kao i za potrebe odgovornih lica za proces upravljanja rizikom.

S obzirom na činjenicu da se oblast sajber bezbednosti brzo razvija, da bi proces upravljanja rizikom bio uspešan, neophodna je i konstantna provera identifikovanih rizika i definisanih mera koje treba primeniti, kao i kontinuirano poboljšanje načina i planova za upravljanje rizicima.

Nacionalni CERT Republike Srbije ne promoviše ili favorizuje bilo koji od korišćenih javnih izvora, među kojima su i komercijalni proizvodi i usluge. Sve preporuke, analize i predlozi dati su u cilju prevencije i zaštite od bezbednosnih rizika.

Izvori:

- SRPS ISO/IEC 27000:2016 Informacione tehnologije – Tehnike bezbednosti – Sistemi menadžmenta bezbednošću informacija
- SRPS ISO/IEC 27005:2011 Informacione tehnologije – Tehnike bezbednosti – Sistemi menadžmenta bezbednošću informacija
- ISO 22301:2019(en) Security and resilience — Business continuity management systems — Requirements
- ISO 22313:2020(en) Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- ISO 31000:2018(en) Risk management — Guidelines
- Studija izvodljivosti uspostavljanja procedura nacionalnog CERT-a i upravljanja sistemom za prijavu incidenta; Okvir plana kontinuiteta poslovanja za CERT platformu