OSNOVE O SUSTAVIMA ZA UPRAVLJANJE SIGURNOŠĆU INFORMACIJA

Igor Smud

CARNet

Igor.Smud@carnet.hr

01/ 6661 725

Sažetak

Važnost postojanja sustava za upravljanje sigurnošću u akademskoj i istraživačkoj zajednici,kakve su pretpostavke bitne za izradu kvalitetnog sustava za upravljanje, a ujedno i način uvođenja i provođenja istog uvijek su nedovoljno razjašnjavani. Ovaj rad nastoji približiti koje su fundamentalne pretpostavke od kojih kreće izrada ovakvog sustava, što je u svakom koraku nužno imati na umu, te na koji način će od ovakvog sustava imati koristi firma u cjelosti.

1. Temeljne pretpostavke

Svijest o potrebi za upravljanjem sigurnošću informacija još je nedovoljno raširena u akademskoj zajednici. Zato je potrebno ukazivati na ozbiljnost potrebe za postojanjem sustavnog upravljanja sigurnošću informacija. No, tamo gdje i postoji inicijativa za postojanjem kvalitetnog i održivog sustava za upravljanje sigurnošću informacija, postoje i mnoge zapreke a koje se najčešće javljaju zbog nerazumijevanja ideje koja se krije iza cijelog takvog sustava.

Neke informacije imaju vrlo velike vrijednosti kako za pojedince, tako i za cijele ustanove jer prenose važne informacije (primjerice o rezultatima istraživanja). Oko informacija su izgrađeni informacijski sustavi koji omogućuju njihovu bolju iskoristivost, dostupnost, obradu, prijenos, itd. Zaštita samo informacija ili samo sustava koji ih okružuju nije dostatna, a dodatno zaštiti informacija i sustava, potrebno je obratiti pažnju i na ljudski faktor koji njima upravlja.

2. Sustav za upravljanje sigurnošću informacija

Dio sustava za upravljanje sigurnošću informacija je sigurnosna politika čiji je cilj odrediti skup pravila za korištenje, održavanje i dizajn informacijskog sustava, odrediti tko može imati kakvu ulogu u tom sustavu, te odrediti pojmove koji su važni. U prvom redu važno je jasno odrediti pravila sigurnosti jer bez toga sigurnosti nema. Svijest i znanje o tim pravilima izrazito je bitno kako bi cijeli sustav uspješno funkcionirao. Nadalje, vrlo je važna podrška uprave za rad sustava, kako bi se svi zahtjevi koje takav sustav nameće mogli provesti.

Jedan od faktora za uspješnu primjenu sigurnosne politike je i znanje o sigurnosnoj politici svih zaposlenika firme. Bez edukacije o politici, njezinim ograničenjima i dopuštenjima, vrlo

lako se može dogoditi da upravljanje cijelim sustavom postane samo sebi svrha. Time se gubi ona početna pretpostavka za stvaranje takvog sustava i cijela stvar dalje nema smisla.

Informacijski sustavi postižu pojedine aspekte sigurnosti na razne načine kao što je na primjer fizičkom zaštitom, pravilima sigurnog korištenja pojedinih informacija ili dijelova sustava, upravljanjem pristupom i ovlastima korisnika. Zato pored politike sigurnosti postoje pravilnici i procedure koje pobliže opisuju zahtjeve na pojedine dijelove informacijskog sustava. Neki pravilnici su na primjer pravilnik o sigurnosi mreže, pravilnik o prihvatljivom korištenju informacijskog sustava, pravilnik o računalnim i primjenskim sustavima. Važno je da pravilnici i procedure u zahtjevima obuhvate aspekte sigurnosti informacija: dostupnost, integritet i povjerljivost, a opet s druge strane da budu provedive.