HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Podizanje svijesti o informacijskoj sigurnosti

CCERT-PUBDOC-2005-11-139

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Opće je poznata činjenica da su ljudski resursi organizacije najveća prijetnja informacijskoj sigurnosti. Oni ugrožavaju informacijske resurse kako slučajnim pogreškama tako i namjernim pokušajima neovlaštenih aktivnosti. Prema podacima Instituta za nacionalnu sigurnost (National Security Institute, SAD) gotovo 75% sigurnosnih incidenata događaju se „iznutra". Kako bi se promijenilo ponašanje i navike zaposlenika, potrebno je intenzivno razmišljati, učiti i djelovati na polju podizanja svijesti o informacijskoj sigurnosti.

Podizanje svijesti o informacijskoj sigurnosti ima za cilj podići osviještenost zaposlenika te ih naučiti određenim znanjima i vještinama o sigurnosti na različitim hijerarhijskim razinama. Nitko unutar organizacije nije i ne smije biti izuzet od programa i treninga ove vrste.

Podizanje svijesti o informacijskoj sigurnosti efikasno je samo ako se planirana, provodi, evaluira i unaprjeđuje prema određenim smjernicama. U sklopu ovakvog programa i treninga zaposlenici se kontinuirano upoznaju s aktualnim temama na području informacijske sigurnosti te ih se navodi na primjereno korištenje informacijskih resursa s ciljem smanjenja rizika od potencijalnih sigurnosnih incidenata.

2. Program i trening podizanja svijesti o informacijskoj sigurnosti

Obrazovanje odnosno učenje jest kontinuiran proces. Ono započinje kao program za podizanje svijesti o informacijskoj sigurnosti, izrasta u trening, ali može se promatrati i kao formalna edukacija. U praksi se vrlo često pojmovi *security awareness program* i *security awareness trening* smatraju istoznačnicama, iako među ovim pojmovima postoji značajna razlika. Radi lakšeg razumijevanja umjesto pojma *security awareness program* koristit će se pojam program, a umjesto pojma *security awareness trening* koristit će se pojam trening.

Program podizanja svijesti o informacijskoj sigurnosti je način usmjeravanja pažnje na informacijsku sigurnost i relevantne aspekte. Provodi se putem prikladnih materijala i tehnika čija je namjena uputiti sve zaposlenike u prepoznavanje sigurnosno relevantnih pojmova i problema te ponašanje u skladu s njima. Tijekom ove aktivnosti, sudionici su samo primatelji informacije. Cilj programa je širokoj publici predstaviti tematiku informacijske sigurnosti na zanimljiv, kreativan i motivirajući način. Ovo je aktivnost kratkog trajanja usmjerena na specifičnu temu ili skup tema koje čine cjelinu. Treba napomenuti kako je provođenje programa aktivnost koja je usmjerena na apsolutno sve zaposlenike i ima veliki utjecaj na organizacijsku kulturu.

Za razliku od programa, trening je formalnija aktivnost koja ima za cilj izgraditi znanja i vještine povezane s informacijskom sigurnošću. Trening predstavlja kontinuiranu aktivnost koja se provodi za određene grupe ljudi. Ovu aktivnost obvezno trebaju proći korisnici informacijskog sustava na svim hijerarhijskim razinama.

Osnovna razlika između treninga i programa jest ta što trening zahtjeva svladavanje određenih znanja i vještina koje korisnicima omogućavaju izvođenje određenih akcija u skladu s definiranim pravilima, dok program zahtjeva da se zaposlenikova pažnja usmjeri na određenu temu ili skupinu tema.

Program i trening imaju i jedanzajednički cilj, a to je kod svakog zaposlenika razviti atribute koji se smatraju kritičnima i kojima treba težiti tijekom obrazovanja. To su razumijevanje, promišljenost i odgovornost. Razumijevanje ukazuje na karakteristiku zaposlenika da razumije informacijsku sigurnost i relevantne pojmove. Promišljenost se odnosi na promišljanje o utjecaju poslovnih i zakonskih propisa te odgovornosti koji iz njih proizlaze. Odgovornost je karakteristika zaposlenika da prepozna sigurnosne incidente, djeluje u skladu s njima te ih prijavi nadležnoj službi u organizaciji.

Program i trening najbolje je usporediti kroz nekoliko atributa kako bi se uvidjele njihove specifičnosti. Atributi su stupanj znanja koje određena aktivnost pruža, cilj obrazovanja koji se želi postići, metode poučavanja koja se mogu koristiti, način testiranja radi utvrđivanja razine postignutih ciljeva te vremenski okvir (Tablica 1).

Program odgovara na pitanje ŠTO? te odgovorima nudi informacije o informacijskoj sigurnosti kao stupanj znanja. Cilj koji se postiže je prepoznavanje i zadržavanje pojmova. Za program se mogu koristiti mediji kao što su prezentacije, video zapisi, brošure, posteri, razni uredski materijal i sl. Testiranje zadržanih informacija provodi se putem odgovora tipa Točno / Netočno ili putem

višestrukog izbora kako bi se identificiralo naučeno. Kada se spominje vremenski okvir programa, tada je to kraktoročno trajanje.

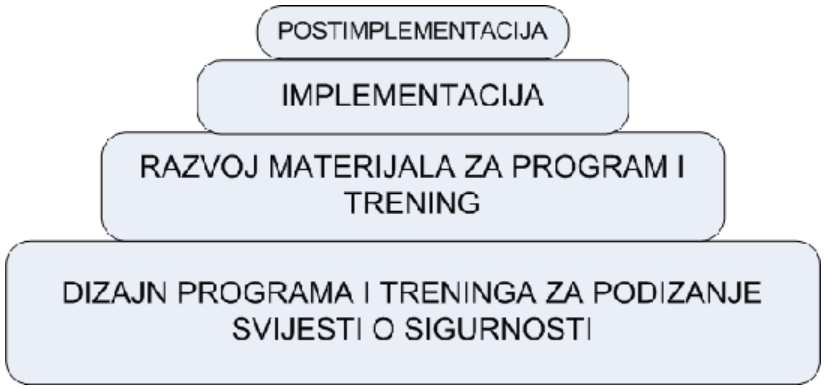
Usporedba komponenti		
Atributi	**Program**	**Trening**
	ŠTO?	KAKO?
Stupanj znanja	Informacija	Znanje
Cilj obrazovanja	Prepoznavanje i zadržavanje	Vještina
Metoda poučavanja	Putem medija: prezentacije, video, brošure, posteri...	Putem praktičnih instrukcija: predavanja, studiji slučaja, praksa...
Testiranje	T/N odgovori, višestruki izbor IDENTIFIKACIJA NAUČENOG	Rješavanje problema PRIMJENA NAUČENOG
Vremenski okvir trajanja	Kratkoročno	Srednje trajanje

Tablica 1: Usporedba programa i treninga

Program i trening namijenjeni su zaposlenicima kako bi se kod njih razvila svijest o tome da zaštite (engl. *Protect*) , detektiraju (engl. *Detect*) i reagiraju (engl. *React*) u svakodnevnom obavljanju poslovnih zadataka.

3. Životni ciklus podizanja svijesti o informacijskoj sigurnosti

Razvoj programa i treninga za podizanje svijesti o informacijskoj sigurnosti odvija se u četiri faze. To su: dizajn programa i treninga, razvoj materijala za program i trening, implementacija programa i treninga te postimplementacijska faza. Svaka faza životnog ciklusa programa i treninga mora biti u skladu s poslovnim ciljevima organizacije. Poslovne potrebe su glavni pokretač kreiranja programa i treninga i one moraju biti zadovoljene na prvome mjestu.
Slika 1 prikazuje faze životnog ciklusa podizanja svijesti o sigurnosti koje su dalje opisane.



Slika 1: Faze životnog ciklusa podizanja svijesti o informacijskoj sigurnosti

3.1. Dizajn programa i treninga

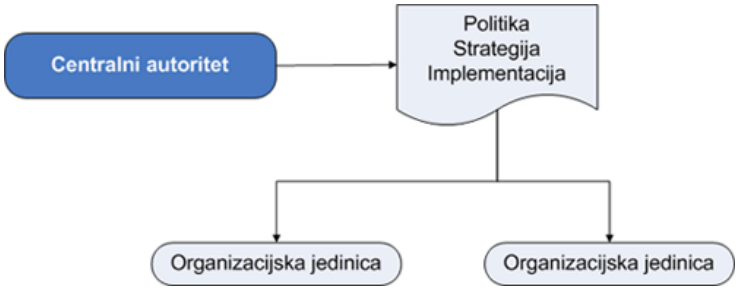
Pitanja na koja je potrebno odgovoriti u fazi dizajna programa i treninga za podizanje svijesti o informacijskoj sigurnosti su: koji se cilj želi postići, kako strukturirati aktivnosti unutar organizacije, kako provoditi procjenjivanje trenutne razine svijesti o sigurnosti, kako razviti strategiju i plan programa i treninga, kako uspostaviti prioritete pri implementaciji programa i treninga, kako postaviti granice kompleksnosti pri razvoju materijala te na koji način financirati program i trening.

3.1.1. Postavljanje cilja

Osnova za daljnje faze životnog ciklusa jeste postavljanje cilja koji se želi postići programom i trenignom. Cilj treba predstavljati i podržavati misiju organizacije.

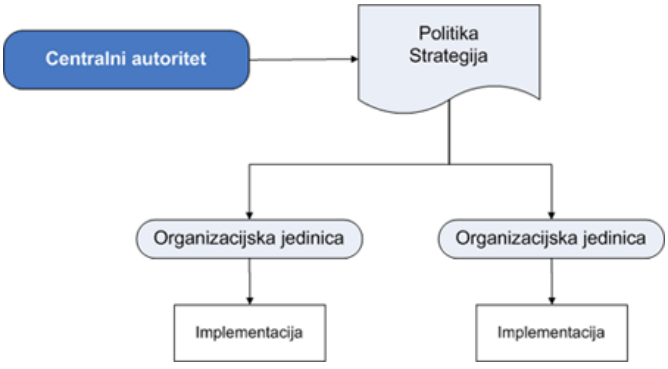
3.1.2. Strukturiranje aktivnosti

Kada se govori o strukturi, ono što organizacije trebaju definirati jest jedan od tri modela upravljanja programom i treningom. Modeli se razlikuju po glavnom tijelu koje će donositi politiku, strategiju, te tijelu koje će implementirati program i trening. Politika upućuje na potrebu provođenja programa i treninga. Odabir odgovarajućeg modela izvodi se prema veličini i geografskoj disperziji organizacije, prema definiranoj organizacijskoj strukturi, ulogama i odgovornostima te prema budžetu.
Prvi model jest centralizirani model koji se sastoji od centralizirane politike, centralizirane strategije te centralizirane implementacije programa i treninga. Karakteristika ovog modela jest što najveću ulogu ima tzv. centralni autoritet koji određuje sve navedene elemente modela za cijelu organizaciju. Komunikacija između centralnog autoriteta i organizacijskih jedinica u ovom modelu je dvosmjerna. Slika 2 prikazuje prvi model.



Slika 2: Centralizirani model upravljanja programom i treningom

Drugi model je djelomično decentraliziran u kojem su politika i strategija centralizirane, a implementacija decentralizirana. Centralni autoritet zadužen je za politiku i strategiju na razini cijele organizacije, a implementacija je delegirana menadžerima u organizacijskim jedinicama koji ujedno vode brigu o financiranju, razvoju materijala, planu provođenja te odgovornostima. Djelomično centraliziran model prikazan je na Slika 3.



Slika 3: Djelomično decentralizirani model upravljanja programom i treningom

Treći model je potpuno decentraliziran model u kojemu je politika centralizirana, a strategija i implementacija decentralizirane. Centrali autoritet razvija politiku, a organizacijske jedinice provode procjenu, razvijaju strategiju i plan provođenja, odlučuju o financiranju, razvoju materijala i implementaciji. Potpuno decentralizirani model prikazuje Slika 4.

Slika 4: Potpuno decentralizirani model upravljanja programom i treningom

3.1.3. Procjena trenutnog stanja svijesti

Provođenje procjene potreba programa i treninga koristi se za određivanje trenutne razine svijesti o informacijskoj sigurnosti u organizaciji. Rezultat procjene ujedno će poslužiti i za uvjeravanje menadžmenta za ulaganje u program i trening te će služiti za procjenu postignute razine svijesti nakon provođenja programa ili treninga. Neke od metoda koje se mogu koristiti prilikom procjene trenutne razine svijesti su intervjui, ankete, revizija postojećih programa, treninga i materijala, revizija sigurnosnih planova, itd. Metode treba odabrati obzirom na organizacijske specifičnosti. Osim klasičnih anketa i intervjua, kao metoda može poslužiti neslužbeni razgovor sa zaposlenicima tijekom pauza ili praćenje sigurnosnih incidenata prije i poslije programa ili treninga.
Tablica 2 prikazuje neke metode koje se koriste kao za prikupljanje informacija i procjenu trenutnog stanja svijesti.

Metode prikupljanja informacija			
Metoda	**Namjena**	**Prednosti**	**Izazovi**
Upitnik, anketa	Pogodno za brzo prikupljanje mnoštva informacija na nenametljiv način.	- može biti anonimno - jeftino - jednostavno za obradu - pogodno za velik broj podataka - postoji puno gotovih materijala	- nisu osobni - potreban je dobar odabir statističkog uzorka
Intervju	Pogodan kada se želi dobiti potpuno razumijevanje nečijeg mišljenja i iskustva.	- daje potpunu sliku i dubinu informacije - razvija se odnos sa sugovornikom - omogućava fleksibilnost	- može trajati duže vrijeme - teško je analizirati odgovore - mogu biti skupi
Revizija dokumentacije	Pogodno za promatranje provođenja programa i treninga bez prekidanja postupka.	- pruža opsežne i povijesne informacije - ne ometa izvođenje programa - sve informacije već postoje	- uzima više vremena od ostalih - nedostatak informacija

Metode prikupljanja informacija			
Metoda	**Namjena**	**Prednosti**	**Izazovi**
Promatranje	Služi prikupljanju informacija o načinu provođenja programa i treninga.	- prikazuje operacije na realan način - prilagođava se događaju tijekom odvijanja	- poteškoće pri interpretaciji ponašanja - kompleksnost pri kategorizaciji promatranja - može utjecati na ponašanje sudionika - skupo
Ciljne grupe	Istraživanje teme u dubinu kroz grupne diskusije.	- brzo i pouzdano donošenje zajedničkih zaključaka - efikasan način za dobivanje detaljnih informacija u kratkom vremenu - pridonosi ključne informacije o programu i treningu	- teška analiza odgovora - potrebna izvrsna osoba za podršku - teškoće pri organizaciji grupe ljude
Studij slučaja	Pogodno za puno razumijevanje iskustava klijenata u programu i treningu i provođenje opširnih ispitivanja kroz komparacija studija.	- potpuno oslikavanje iskustava - jako sredstvo za prikazivanje programa i treninga ostalim klijentima	- potrebno duže vrijeme za prikupljanje, organiziranje i opisivanje slučaja

Tablica 2: Metode za prikupljanje informacija

3.1.4. Politika i strategija

Procijenjeno stanje trenutne razine svijesti temelj je za razvoj strategije i plana programa i treninga. Plan programa i treninga se treba vezati na politiku koja zahtjeva da se program i trening provedu, a sadrže opseg programa i treninga, uloge i odgovornosti, ciljeve koji se žele postići, ciljanu publiku, obvezne teme koje se trebaju slušati, teme koje će se obraditi, način evaluacije i ažuriranja materijala te frekvenciju provođenja programa i treninga. Pod obvezne teme mogu spadati zakonske regulative, politike i procedure organizacije, sustav za upravljanje informacijskom sigurnošću ukoliko ga organizacija ima, dijeljenje informacija, antivirusna zaštita, klasifikacija informacija, itd. Pod ostale teme mogu se uključiti sigurnosni alati, procjena rizika, kriptografija i sl.

3.1.5. Određivanje prioriteta

Nakon izrade plana, potrebno je definirati raspored prioriteta. Raspored prioriteta određuje koji će se konkretno program i trening provoditi. Ovaj korak će se najviše razlikovati od jedne do druge organizacije, dok ostali mogu imati nekih zajedničkih karakteristika.

3.1.6. Postavljanje granice kompleksnosti

Za svaki program i trening potrebno je postaviti granice kompleksnosti koje će definirati razvoj materijala. Materijali se trebaju razvijati zadovoljavajući dva osnovna kriterija, a to su hijerarhijska razina na kojoj se nalazi ciljana publika unutar organizacije te potrebno znanje i vještine koje odgovaraju toj hijerarhijskoj razini. Ta dva kriterija moraju biti poznata prije početka razvoja materijala. Važnost definiranja kompleksnosti dolazi naročito do izražaja kod razvoja materijala za trening, jer cilj treninga jest razviti samo one vještine koje su relevantne i potrebne.

3.1.7. Financiranje

Posljednji, ali najvažniji korak ove faze jest financiranje koje mora biti razmatrano već u fazi planiranja. Prvi zadatak jest uvjeriti menadžment u opravdanost ovih aktivnosti na način da im se ukaže na financijske iznose koji se troše za tehničku sigurnost, kolika je prava vrijednost organizacijskih informacijskih resursa, što znači izgubiti ugled zbog sigurnosnog incidenta te što znači imati konkurentsku prednost. Pravilnim prikazom navedenih stavki, financiranje podizanja svijesti o sigurnosti neće biti problem.

3.2. Razvoj materijala

Dizajn programa i treninga za podizanje svijesti o informacijskoj sigurnosti uzeo je u obzir sve bitne elemente koji se odnose na politiku, strategiju, planiranje i implementaciju programa. Razvoj materijala jest slijedeća faza životnog ciklusa programa i treninga. Osnovna svrha koju materijali moraju opravdati jest da se informacije i vještine koje se njima prenose zaista mogu integrirati u poslovne aktivnosti zaposlenika. Ukoliko zaposlenici ne mogu informacije i vještine koristiti u stvarnim situacijama, neće biti postignut cilj programa i treninga. Također, materijal mora imati točno određenu namjenu. Prilikom razvoja materijala treba voditi računa o tome da li se on razvija za program ili za trening podizanja svijesti o sigurnosti.

3.2.1. Materijali za program

Prilikom razvoja materijala za program preporučljivo je u svakom trenutku imati na umu pitanje „Što je to što svi zaposlenici trebaju znati o informacijskog sigurnosti?“ Odgovorom na ovo pitanje ujedno se rješava popis tema koje će biti obuhvaćene materijalom. Postoji mnoštvo gotovih materijala, ali na engleskom govornom području, koji mogu biti uključeni u program podizanja svijesti o sigurnosti. Izvor dobivanja materijala mogu biti profesionalne organizacije koje se bave izradom materijala, razne konferencije, seminari i tečajevi te razvoj unutar organizacije. Materijal za program može biti kreiran na način da pokriva samo jednu temu ili uključuje više tema koje se međusobno nadopunjuju i čine cjelinu. Količina tema koju će materijal pokrivati treba biti prilagođena tipu materijala, npr. poster može sadržavati samo jednu temu, dok prezentacija može uključivati više tema.

3.2.2. Materijali za trening

Pitanje koje treba imati na umu kada se kreće u razvoj materijala za trening je „Kojim vještinama želimo naučiti korisnike?“ Nakon odabira odgovarajućih tema, traži se odgovarajući izvor materijala. Izvor može biti profesionalna organizacija ili se materijal može razvijati unutar organizacije. Oba pristupa imaju svojih prednosti i mana. Ukoliko se materijali razvijaju unutar organizacije (tzv. *in-house*) tada treba procijeniti da li postoje odgovarajući resursi za razvoj materijala, kakav je odnos troškova vlastitih resursa u odnosu na vanjskog izvođača usluge itd. S druge strane, kod najma usluge treba voditi računa o tome da li će gotovo rješenje zaista zadovoljiti potrebe koje organizacija ima.

3.2.3. Ciljana publika

Bitnu ulogu pri razvoju materijala svakako ima i ciljana publika. Publika se općenito može grupirati u dvije osnovne skupine, a to su tehnička i netehnička skupina polaznika programa i treninga. U tehničku skupinu spadaju stručnjaci za informacijsku sigurnost, administratori, programeri, sistem inženjeri i slične funkcije koje imaju direktnu vezu s informatičkim odjelom organizacije te napredni korisnici informacijskog sustava (engl. *power users*).

Tehnička skupina spada u ciljanu publiku koju treba obrazovati jer se ova skupina zaposlenika obično unaprijed stavlja u skupinu ljudi koja razumije informacijsku sigurnost te se od njih očekuje da implementiraju i rade većinu tehničkih kontrola. Program i trening za ovu skupinu pomoći će im da poboljšaju razumijevanje inforamcijske sigurnosti i pomoći pri uvođenju odgovarajućih tehničkih kontrola u sustav organizacije.

Netehničku skupinu čine menadžeri i svi ostali zaposlenici čiji posao nije informatičke prirode. Menadžeri prije svega moraju demonstrirati svoju podršku programu i treningu kada je u pitanju informacijska sigurnost. Općenito, menadžeri imaju bitnu ulogu u nadgledanju svih aktivnosti te su uključeni u kontrole povezane s informacijskom sigurnošću.

Svi ostali zaposlenici ipak su prava ciljana publika jer koriste informacijski sustav i rade s poslovnim informacijama. Oni trebaju biti potaknuti kako bi vodili računa o informacijskoj sigurnosti, sigurnosnim politikama i relevantnim pojmovima i procedurama, a s kojima trebaju biti upoznati kroz program za podizanje svijesti.

3.3. Implementacija

Faza implementacije slijedi nakon što su sve prethodne faze izvršene u potpunosti. Procjena trenutnog stanja svijesti je temelj nakon kojeg slijedi strategija koja mora biti upotpunjena planom programa i treninga za podizanje svijesti o sigurnosti te konačno moraju biti razvijeni materijali za obje aktivnosti. U fazi implementacije ističu se dva koraka. Prvi korak je rasprava o implementaciji kroz organizaciju kako bi se osigurali svi potrebni resursi te se zaposlenici upoznali s namjerom. Komunikacijske metode koje se mogu koristiti za promociju implementacijske faze mogu biti različite. Organizacije mogu koristiti Intranet (web stranice) kako bi istaknuli važnost, potrebu te značenje programa i treninga. Uobičajeni način komunikacije jest tzv. „oči u oči" gdje se sa zaposlenicima razgovara na sastancima. Također, mogu se koristiti i prezentacije.
Drugi korak predstavlja izbor tehnika za isporuku materijala. Razlikujemo tehnike koje su pogodne za isporuku programa podizanja svijesti o sigurnosti te treninga za podizanje svijesti o sigurnosti.
Za program se obično koriste poruke na različitim uredskim materijalima kao što su olovke, flomasteri, post-it listići, mediji za prijenos podataka, knjiške oznake, satovi, karte, posteri, itd.; zaštitnici zaslona, ispisane poruke koje se dostavljaju na stol, poruke elektroničke pošte, video zapisi, maskote i sl.
Kod treninga koriste se drugačije tehnike. One se biraju tako da zadovoljavaju određene kriterije kao što su jednostavnost korištenja, skalabilnost, mogućnost praćenja razine zadovoljenja vještina itd. Neke od tehnika su interaktivni video trening, online trening, trening na računalima, trening s instruktorima i sl.

3.4. Postimplementacija

Svaki program i trening za podizanje svijesti o sigurnosti s vremenom zastarjeva te prestaje biti u skladu s poslovnim ciljevima organizacije. Ciljevi su također podložni promjenama kao što se s vremenom mijenja i trenutna razina svijesti o sigurnosti. Svi ti promjenjivi elementi zahtijevaju redovno ažuriranje programa i treninga zbog čega je faza postimplementacije također jedna od bitnih faza i spada u životni ciklus podizanja svijesti o sigurnosti. Postimplementacija ima za cilj kontinuirano poboljšanje programa i treninga. Nakon prve implementacije programa potrebno je uspostaviti sustav za praćenje efektivnosti programa te sukladnosti s planom. Pri tom je potrebno vršiti evaluaciju i koristiti povratne informacije koje će dodatno usmjeravati proces unaprjeđenja. Evaluacija će pomoći pri sakupljanju informacija o zadovoljstvu zaposlenika prezentiranim materijalima, obrađenim temama te ostalim relevantnim podacima za organizaciju vezanim uz unapređenje programa i treninga.

4. Zaključak

Obrazovanje o informacijskoj sigurnosti je kontinuirani proces koji privlači sve više pozornosti u poslovnim okruženjima. Predstavlja vrlo važnu točku svake organizacije kao komponenta sustava za upravljanje informacijskom sigurnošću. Svaka organizacija treba biti svjesna da je sigurnost informacijskih resursa efikasna samo ako predstavlja dio odgovornosti svakog zaposlenika. U praksi organizacije polažu vrlo malo pažnje programima i treninzima o podizanju svijesti, iako oni predstavljaju značajan dio ulaganja u informacijsku sigurnost.
Podizanje svijesti o sigurnosti jedini je pravi način održavanja zadovoljavajuće razine sigurnosti, jer utječe na ponašanje krajnjih korisnika i mijenja kompletnu organizacijsku kulturu. Nikada ne treba zaboraviti da je cilj programa i treninga proizvesti relevantne i potrebne vještine i kompetencije.

5. Literatura

[1] NIST Special Publication 800-16: Information Technology Security Training Requirements: A Role – and Performance-Based Model
[2] NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program
[3] NIST Special Publication 800-55: Security Metrics Guide for Information Technology Systems
[4] National Security Institute: Improving Security from the Inside Out