Informacijska sigurnost

Certifikati iz područja informacijske sigurnosti

LSS-PUBDOC-2011-01-012

Laboratorij za sustave i signale

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom LSS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i LSS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu security@LSS.hr.

O LSS-u

LSS (Laboratorij za sustave i signale) je kolijevka u kojoj se 1991. godine rodila ideja o hrvatskom Internetu. Prvi ljudski resursi tima koji je doveo Internet u Hrvatsku dolazili su upravo iz LSS-a [www.LSS.hr].

Još u ranoj razvojnoj fazi CARNet-a (eng. Croatian Academic and Research Network) i Interneta u Hrvatskoj, oni su bili izloženi brojnim napadima. Najveći se, međutim, dogodio 1995. godine. Ovaj događaj smatra se rođenjem računalne sigurnosti u Hrvatskoj.

Sve do današnjega dana, LSS [security.LSS.hr] je educirao brojne sigurnosne stručnjake i timove. Budući da je dio zagrebačkog Sveučilišta, LSS smatra svojom dužnošću širiti znanje i informacije iz područja informacijske sigurnosti i time doprinositi sigurnosti informacijskih sustava na nacionalnoj i globalnoj razini.

LSS je pomogao u osnivanju nacionalnog centra za informacijsku sigurnost CARNet CERT-a i aktivno snabdijeva javnost s najnovijim informacijama o sigurnosnim ranjivostima, događajima i alatima. Točnije, LSS donosi:

- sigurnosne preporuke na dnevnoj bazi
- recenzije sigurnosnih alata na mjesečnoj bazi
- dokumente o sigurnosnim temama na mjesečnoj bazi
- servis za automatsko otkrivanje lažnih poruka elektroničke pošte (eng. hoax)

Osim akademskih, LSS također pruža i komercijalne usluge klijentima sa područja akademskih zajednica, vladinih i nevladinih te komercijalnih organizacija. LSS pruža usluge:

- upravljanja sigurnošću
- provjere sigurnosti
- zaštite informacijskih sustava
- rješavanja sigurnosnih incidenata
- edukacije.

Prava korištenja

Sadržaj

1. Uvod

Glavni cilj informacijske sigurnosti je zaštita dostupnosti, povjerljivosti i cjelovitost informacija. Pod time se misli na to da informacije moraju biti točne i uvijek dostupne onima koji imaju pravo koristi ih. Prikupljanje, obrada i čuvanje informacija sve su više regulirani zakonima i uredbama, koji obvezuju sve organizacije da se pobrinu za zaštitu korištenih informacija. Najpoznatiji međunarodni standardi koji se bave informacijskom sigurnošću i na kojima su certifikati iz područja informacijske sigurnosti zasnovani su ISO 17799 i ISO 27001. Ti se standardi stalno mijenjaju i dorađuju kako bi bili dio sustava u kojem su usklađeni s drugim standardima (primjerice sa standardom ISO 9001, koji se bavi upravljanjem kvalitetom poslovanja) i međusobno. Standard ISO 27001 se bavi uspostavom sustava upravljanja informacijskom sigurnošću, koji se označava kraticom ISMS (eng. *Information Security Management System*). U tom standardu su određeni ciljevi koje organizacija treba postići kako bi imala učinkovit sustav zaštite svojih informacija. ISO 17799 se bavi načinima, postupcima i najboljim praksama pomoću kojih se ti ciljevi mogu postići. Iz tog se razloga obično kaže da se standard ISO 27001 bavi normama, a ISO 17799 provjerama pomoću kojih se praktično mogu ispuniti zahtjevi norme.

Prema općenito prihvaćenoj definiciji, certifikat je službena potvrda da osoba posjeduje određena znanja i vještine. Osim u računalnoj industriji kao dokaz poznavanja određenih proizvoda i tehnologija, certifikati su rašireni i u drugim djelatnostima kao što su zdravstvo, pravosuđe te prosvjeta. U tim je djelatnostima posjedovanje određenih certifikata nužno za bavljenje tim poslom. Najčešće se certifikati ne odnose na poznavanje općih znanja te nisu zamjena za formalno školovanje. Certifikacijskim ispitima se ispituje poznavanje određenih konkretnih proizvoda, načina rada i tehnologija. Iz tog je razloga trajanje valjanosti certifikata najčešće na razdoblje od jedne do tri godine. Da bi se produžilo trajanje certifikata, potrebno je ponovno položiti certifikacijski ispit. Certifikata iz područja informacijske sigurnosti ima vrlo mnogo i u ovom dokumentu su opisani najrenominiraniji među njima (poglavlje: „Poznati certifikati iz područja informacijske sigurnosti“), kao i najvažnije organizacije koje ih dodjeljuju (poglavlje: „Organizacije koje dodjeljuju certifikate“).

2. Čemu služe certifikati?

Pojedinci i poslodavci imaju višestruke koristi od certifikata i certificiranja, a neke od koristi za pojedince navedene su u nastavku:

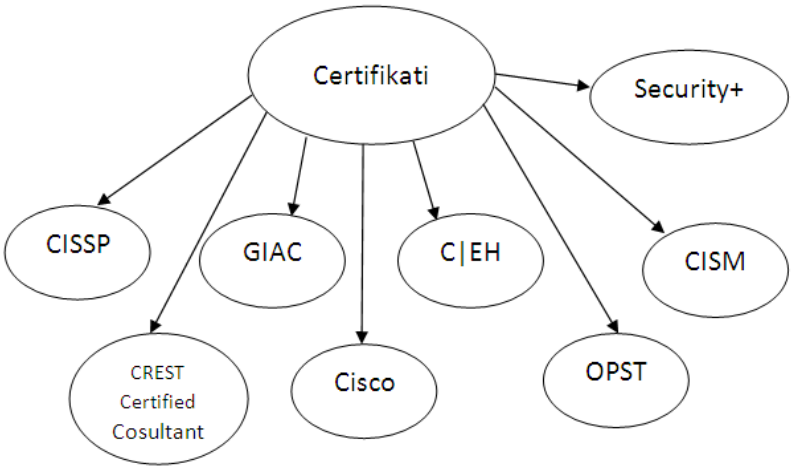
- **Lakše zaposlenje**. Neki poslodavci i tvrtke traže posjedovanje određenog certifikata prilikom raspisivanja natječaja za neko radno mjesto. Certifikat je važan element poslodavcu za procjenu kandidata prije nego ih pozovu na razgovor. Općenito, osoba s certifikatom ima veće šanse pronaći posao.
- **Bolja plaća**. Poslodavci su spremni više platiti osobe s certifikatom jer on služi kao dokaz većeg znanja, iskustva i produktivnosti.
- **Napredak u karijeri**. Uz veću zaradu, certifikat pojedincu otvara veće šanse za dobivanje boljeg posla i daljnji napredak u karijeri.
- **Dokaz o poznavanju tehnologije**. Certifikat poslodavcu jamči da znanje osobe prati i odgovarajuće iskustvo potrebno da bi se određeni certifikat stekao.
- **Dodatna podrška proizvođača opreme**. Obično uključuje pristup proizvođačevoj službi podrške, pristup programskim nadogradnjama i priliku za testiranje najnovije inačice programske podrške.

Najvažnije koristi koje poslodavci imaju od certificiranja su:

- **Jednostavnija selekcija kandidata**. Certifikat objektivno jamči da osoba uz formalnu izobrazbu posjeduje i konkretno znanje koje je potrebno u radu.
- **Produktivnost osoblja s certifikatom**. Osobe s certifikatom mogu podržavati veći broj korisnika i spriječiti skupe prekide u radu računala i računalnih mreža.
- **Osobe s certifikatom dobivaju podršku proizvođača opreme**. Izravnu korist ima poslodavac jer i on dobiva pristup službi podrške i novim programskom nadogradnjama.
- **Osobe s certifikatom rjeđe mijenjaju posao**. Osoblje cijeni poslodavce koji investiraju u njih i takvi poslodavci imaju koristi od školovanog osoblja. Birajući posao, osoblje bira poslodavca koji će se brinuti za razvoj njihove karijere.
- **Osobe s certifikatom znaju iskoristiti sve mogućnosti opreme**. Osoba s certifikatom raspolaže znanjima o najnovijim mogućnostima neke opreme te u kojim situacijama se one mogu koristiti. Računalna oprema je strateška investicija i treba je povjeriti onome tko najbolje zna s njome raditi.

3. Poznati certifikati iz područja informacijske sigurnosti

Certifikata iz područja informacijske sigurnosti, kao i organizacija koje ih dodjeljuju, ima jako puno. Svi ti certifikati su međusobno slični, ali svaki donosi i određene specifičnosti. Sličnost između certifikata se očituje u tome da je svima primarni cilj dokazati sposobnost osobe u području zaštite informacijske sigurnosti. Razlike postoje u specijaliziranim znanjima iz područja informacijske sigurnosti koje certifikat donosi, kao i u cijeni te načinu polaganja. Poznatije organizacije koje dodjeljuju certifikate su CompTIA+, Cisco Systems, EC-Council, SANS Institute, ISACA, (ISC)^2, ISECOM i CREST. U nastavku su navedeni i opisani neki od najpopularnijih certifikata iz područja informacijske sigurnosti (slika 1) koje dodjeljuju ove organizacije dok su kasnije u tekstu pobliže prikazane spomenute organizacije za certificiranje. Certifikati koje objavljuju navedene organizacije su vrlo traženi te okupljaju najveći broj certificiranih ljudi. U nastavku su navedene cijene certifikata te postoji li mogućnost njihovog polaganja u Hrvatskoj. Uz polaganje ispita za određeni certifikat najčešće se nudi i mogućnost edukacije prije same certifikacije. Edukacija se najčešće sastoji od predavanja i vježbi koje se mogu naći i na Internetu te od praktičnog dijela za koji se mora prisustvovati tečaju, nažalost najčešće izvan Hrvatske.



Slika 1. Podjela certifikata iz područja informacijske sigurnosti
Izvor: LSS

3.1. Certified Information Systems Security Professional

Certified Information System Security Professional (CISSP) je nezavisan certifikat iz područja informacijske sigurnosti (slika 2) kojeg dodjeljuje *International Information System Security Certification Consortium* poznatiji kao (ISC)^2. Riječ je o neprofitabilnoj organizaciji osnovanoj 1989. godine kojoj je cilj razvijanje standardnog programa certifikacije koji bi educirao i certificirao osobe i organizacije na području informatičke sigurnosti. CISSP certifikat ima više od 63 tisuće certificiranih osoba u 138 zemalja. CISSP znanja su zasnovana na onome što (ISC)^2 naziva *Common Body of Knowledge* (CBK). Prema (ISC)^2, CBK je zbirka tema i principa vezanih uz informacijsku sigurnost koji omogućuju razumijevanje i rješavanje većine sigurnosnih problema. Domene znanja koje sadrži CBK te koje ima osoba koja je certificirana CISSP certifikatom su:

- provjera pristupa sustavu ili mreži,
- sigurnost pri razvijanju programa,
- kontinuitet planiranja (planiranje u svrhu zaštite od sigurnosnih prijetnji) i planiranje oporavka nakon sigurnosnog incidenta,
- kriptografija (osnovni koncepti i algoritmi, kriptoanalize, digitalni potpisi),
- upravljanje informacijskom sigurnošću i rizicima,
- propisi, sukladnosti i prava u međunarodnoj informacijskoj sigurnosti, kao i uvid u lokalna prava na području na kojem se certifikat izdaje,

- sigurnost operacija koje rade s informacijama,
- fizička sigurnost (sigurnost okruženja),
- arhitektura i dizajn sigurnosti te
- sigurnost mreže i telekomunikacija.

Uvjeti koje kandidat za CISSP certifikat mora zadovoljiti su:

- najmanje 5 godina radnog iskustva iz najmanje dvije domene koje propisuje CBK. U jednu godinu radnog iskustva može se uračunati četverogodišnja fakultetska diploma iz područja informacijske sigurnosti ili posjedovanje nekog drugog certifikata iz informacijske sigurnosti izdanog od druge organizacije za certifikaciju,
- prolazak CISSP ispita (700 od mogućih 1000 bodova, nema negativnih bodova).

CISSP certifikat traje 3 godine i nakon toga je potrebno ponovno položiti certifikacijski ispit. Cijena ispita je oko 90 € i ispit se ne može položiti u Hrvatskoj. Cijena potpunog tečaja s ispitom prelazi 200 €.

Više informacija o CISSP certifikatu može se pronaći na stranicama (ISC)[2]:

https://www.isc2.org/cissp/default.aspx

Slika 2. Logo certifikata CISSP
Izvor: isc2.org

3.2. Global Information Assurance Certification

Global Information Assurance Certification (GIAC) su certifikati iz područja informacijske sigurnosti (slika 3) koje je utemeljio *SANS Institute (eng. SysAdmin, Audit, Networking, and Security)*, institut koji se bavi sigurnošću u računarstvu i informatici. GIAC je certifikat kojim se dokazuje sposobnost organizacije i njezinih informatičkih stručnjaka na području računalne, mrežne i programske sigurnosti. Uključuje certifikate iz više od 10 specifičnih grana vezanih za teoriju i praksu informacijske sigurnosti. Po statistikama koje GIAC i *SANS Institute* navode certifikatom je certificirano više od 30 tisuća osoba i organizacija diljem svijeta. GIAC certificiranje pokriva sljedećih 5 disciplina:

- **administracija informacijske sigurnosti** (eng. *Security administration*) - obuhvaća upravljanje rizicima, oporavak od sigurnosnih pogrešaka, kontinuitet planiranja (planiranje u svrhu zaštite od sigurnosnih prijetnji) te praksu zaštite od sigurnosnih propusta i pogreški,
- **upravljanje sigurnošću** (eng. *Security management)* - obuhvaća znanja iz tehničkog dijela informacijske sigurnosti kao što su sigurnost sustava, mreže i mrežnih programa (Wireshark, dSniff i sl.),
- **forenzika** (eng. *Forensics*) - obuhvaća primjenjivanje znanja iz zakonski dopustivih i nedopustivih dijela vezanih za informacijsku sigurnost,
- **revizija informacijskih sustava** (eng. *IT audit*) - omogućuje stjecanje znanja o normi ISO 17799 i njenoj praktičnoj implementaciji u bilo koju organizaciju te
- **sigurnost programa** (eng. *Software Security*) - obuhvaća znanja potrebna za pisanje sigurnosno prihvatljivih programa.

Certifikat GIAC se dijeli na „*Silver*“ i „*Gold*“ razine. „*Silver*“ razina je niža i zahtjeva prolazak 2 ispita iz informacijske sigurnosti, dok „*Gold*“ razina također zahtjeva prolazak oba spomenuta ispita te prolazak ispita koji obuhvaća praktične probleme (npr. otkrivanje neovlaštenog pristupa sustavu) iz područja informacijske sigurnosti. Pismeni ispiti za svaku disciplinu sadrže 150 pitanja i potrebno je točno odgovoriti na njih 100-110 (nema negativnih bodova), ovisno o ispitu, u vremenu od 4 sata. Poredak kojim se certificira je nebitan, dakle nema preduvjeta za certificiranje pojedine discipline. Cijena samog ispita iznosi 450 $, dok potpuna edukacija s ispitom košta od 600 do 3000 $, ovisno o disciplini i razini. Više informacija o GIAC certificiranju može se naći na adresi:

http://www.giac.org/

Slika 3. Logo certifikata GIAC
Izvor: giac.org

3.3. Certified Ethical Hacker

Certified Ethical Hacker (C|EH) je profesionalni certifikat (slika 4) kojeg dodjeljuje organizacija *International Council of E-Commerce Consultants* (EC-Council). Etički haker je osoba koju organizacija zapošljava da se probije u njenu mrežu ili računalni sustav koristeći jednake metode kao i stvarni napadač. To se radi u svrhu pronalaska i popravka računalnih sigurnosnih ranjivosti. Nelegalno hakiranje (neovlašteni pristup računalnim sustavima) je zločin, ali etičko hakiranje nije i postoje osobe koje su certificirane za taj posao. Etičkih hakera s certifikatom C|EH (po statistikama *EC-Councila*) u svijetu ima preko 20 tisuća. Certifikat se može dobiti nakon 2 godine radnog iskustva u informacijskoj sigurnosti te nakon prolaska C|EH kvalifikacijskog ispita. Neka od znanja koja C|EH certifikat uključuje su:

- **Otkrivanje upada** (eng. *Intrusion detection*) - otkrivanje i sprječavanje neovlaštenog pristupa računalnom sustavu ili mreži,
- **Stvaranje okruženja** *(eng. Policy Creation)* - strategija stvaranja sigurnog okruženja te edukacija vezana uz moguće napade na sustav,
- **Socijalni inženjering** (eng. *Social engineering*) - manipulacija ljudima (trikovi, lažna predstavljanja, …) u svrhu dobivanja potrebnih informacija za neovlašten pristup sustavu (disciplina koju je popularizirao Kevin Mitnick, jedan od najpoznatijih bivših hakera),
- **DDoS napadi** (eng. *Distributed Denial of Service attacks*) - napadi na web stranice s više računala posebno konstruiranim zahtjevima dok se poslužitelj ne uspori toliko da mu se više ne može pristupiti,
- **Preljev međuspremnika** (eng. *Buffer overflow*) - anomalije nastale kad program, pišući u međuspremnik, prekorači njegove granice i prebriše memoriju te
- **Stvaranje zlođudnih programa** (eng. *Virus creation*) - stvaranje virusa, crva ili bilo kakvog drugog zlođudnog programa.

Za dobivanje certifikata C|EH potrebno je položiti jedan od dva moguća ispita: Exam 312-50 ili Exam EC0-350. Ispit Exam 312-50 predstavlja osnovni ispit za etičkog hakera I njega je moguće proći i bez treninga u EC-Councilu, ali je tada potrebno imati najmanje 2 godine radnog iskustva na području informacijske sigurnosti. Za prolazak ispita za naprednog etičkog hakera nužno je obaviti trening u EC-Councilu prije nego je uopće moguć izlazak na ispit. Za prolazak na ispitima potrebno je ostvariti najmanje 70% bodova, a ukupno ima 150 pitanja i vrijeme pisanja je 3 sata. Postoji mogućnost polaganja C|EH ispita u Hrvatskoj, a pojedinosti o tome su navedene u

poglavlju 5. Ponovna certifikacija potrebna je nakon 3 godine. Ostale informacije o C|EH certifikatu mogu se pronaći na stranici EC-Councila:

http://www.eccouncil.org/certification/certified_ethical_hacker.aspx

Slika 4. Logo certifikata C|EH
Izvor: cehcbt.com

3.4. Security+ Certification

Security+ certifikat (slika 5), kojeg dodjeljuje organizacija CompTIA+, je nezavisan internacionalni certifikat koji dokazuje kompetenciju osobe ili organizacije na polju računalne tehnologije. Preciznije rečeno, certifikat dokazuje znanje iz područja sigurnosti sustava, mrežne infrastrukture, provjere pristupa i organizacijske sigurnosti. Prema podacima koje iznosi CompTIA+, *Security+* certifikat trenutno posjeduje više od 45 tisuća ljudi u svijetu. Znanja i vještine koje se stječu certifikatom *Security+* su navedena u nastavku:

- **Provjera pristupa** (eng. *Access control*) koja obuhvaća:
  - Razlikovanje MAC/DAC/RBAC (*Mandatory Access Control* - obvezna kontrola pristupa*, Discretionary Access Control* – proizvoljna kontrola pristupa*, Rule based Access Control* – kontrola pristupa na osnovu uloga) provjera pristupa,
- **Autentikacija** (eng. *Authentication*) obuhvaća:
  - Znanje u konfiguriranju autentikacije za sustav.
  - Razlikovanje tipova autentikacije (CHAP, *Username/Password,* tokeni, biometrija itd.) i kriptologije korištene u njima.
- **Servisi i protokoli** koji obuhvaćaju:
  - Razlikovanje bitnih od nebitnih servisa i protokola,
- **Napadi na sustav** koji obuhvaćaju:
  - DoS/DDoS napadi,
  - *Back door* napadi (autor programa ostavlja slobodan ulaz u program, tzv. stražnja vrata),
  - *Password Guessing* (pogađanje lozinke za ulaz u sustav),
  - *Brute Force* (napad koji ne staje dok se ne probije lozinka) te
- **Socijalni inženjering**.

Ispit za certifikat *Security+* se sastoji od 100 pitanja, traje 90 minuta i za prolazak na ispitu potrebno je ostvariti 750 od mogućih 900 bodova (bez negativnih bodova). Radno iskustvo i predznanja za dobivanje ovog certifikata nisu potrebni, ali CompTIA+ preporuča određeno predznanje iz informacijske sigurnosti, položen certifikat Network+ (certifikat kojim se dokazuju znanja iz područja računalnih mreža) i 2 godine radnog iskustva iz područja informacijske sigurnosti. Certifikat *Security+* traje 3 godine i nakon toga ga je potrebno obnoviti. O *Security+* certifikatu više se može saznati na adresi:

http://www.comptia.org/certifications/listed/security.aspx

Slika 5. Logo certifikata Security+
Izvor: comptia.org

3.5. Certified Information Security Manager

Certified Information Security Manager (CISM) je certifikat za menadžere u informacijskoj sigurnosti (slika 6) kojeg dodjeljuje organizacija *Information System Audit and Control Association* (ISACA). Prema podacima iz 2003. godine, koje navodi ISACA, CISM certifikatom je certificirano preko 13 tisuća ljudi. Ono što CISM certifikat razlikuje od ostalih je to što je on namijenjen pojedincima koji upravljaju, projektiraju, nadgledaju i ocjenjuju informacijsku sigurnost organizacije. Certifikat CISM, kako navodi organizacija ISACA, pruža znanja iz sljedećih područja:

- Upravljanje informacijskom sigurnošću (eng. *Information security governance*),
- Upravljanje rizikom (eng. *Information risk management*),
- Razvoj programa informacijske sigurnosti (eng. *Information security program development*),
- Upravljanje programom informacijske sigurnosti (eng. *Information security program management*) te
- Upravljanje i odgovor na propuste u informacijskoj sigurnosti (eng. *Incident management and response*).

U svrhu dobivanja CISM certifikata osobe moraju proći pismeni ispit i moraju imati najmanje 3 godine radnog iskustva u informacijskoj sigurnosti. Ispit se sastoji od 200 pitanja i potrebno je sakupiti 450 od ukupnih 800 bodova (nema negativnih bodova) u vremenu od 4 sata. Cijena certifikata CISM iznosi oko 70€, a sam certifikat traje 3 godine. Stranica na kojoj se može dobiti više informacija o CISM certifikatu dana je u nastavku:

http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx

Slika 6. Logo certifikata CISM
Izvor: isaca.org

3.6. OSSTMM Professional Security Tester

OSSTMM (*Open Source Security Testing Methodology Manual*) Professional Security Tester (OPST) je certifikat koji dokazuje da osoba ima znanja potrebna da bude ispitivač informacijske sigurnosti (slika 7). OSSTMM je metodologija za izvedbu provjere informacijske sigurnosti. OPST certifikat izdaje *Institute for Security and Open Methodologies* (ISECOM). OPST certifikat je potreban osobama koje žele steći i dokazati znanja iz područja provjere mreža i mrežnih programa, etičkog hakiranja te udaljenog pristupa sustavu. Za OPST certificiranje se najčešće odlučuju revizori i inženjeri informacijske sigurnosti, inženjeri mreža, administratori informacijskih sustava i slični. Po ISECOM-ovim statistikama, certifikat OPST trenutno ima preko 15 tisuća ljudi u

svijetu. Osobe certificirane certifikatom OPST, kako navodi ISECOM, imaju sljedeća znanja i vještine iz područja informacijske sigurnosti:

- izvođenje sigurnosnih provjera pomoću metodologije OSSTMM,
- utvrđivanje prava korisnika sustava i mreže putem javnih servisa,
- određivanje vrste *hostinga* („posluživanja“) na mreži (*free, shared, dedicated*),
- otkrivanje aktivnih upada u sustav ili mrežu,
- ispitivanje brzine i učinkovitosti mreže,
- uočavanje anomalija i pogrešaka na sustavu i mreži,
- korištenje mrežnih analizatora (Wireshark, tcpdump, dSniff,…),
- raspoznavanje servisa, programa i protokola u sustavu,
- sposobnost prepoznavanja poznatih sigurnosnih ranjivosti i njihov popravak te
- sposobnost brzog prepoznavanja sustava i njegove inačice (eng. *fingerprinting*).

Za dobivanje OPST certifikata organizacija ISECOM preporuča predznanja iz mrežnih protokola, sigurnosnih programa i uređaja te osnovno razumijevanje operacijskih sustava Linux i Windows. Ispit se sastoji od 140 pitanja i za certifikat je potrebno sakupiti 60% bodova u vremenu od 4 sata. Specifičnost ovog certifikata je što se ne može steći bez položenog treninga. Cijena treninga i ispita iznosi oko 2500 $ i na žalost ne postoji mogućnost certifikacije u Hrvatskoj (kao najbliže certifikacijsko mjesto navodi se Krakow). Više o OPST certifikatu može se saznati na sljedećoj adresi:

http://www.isecom.org/projects/opst.shtml

Slika 7. Logo certifikata OPST
Izvor: isecom.org

3.7. CREST Certified Consultant

CREST Certified Consultant je certifikat koji dokazuje da osobe imaju znanje, vještine i iskustvo u razumijevanju potencijalnih ranjivosti i ostalih rizika u informacijskim sustavima i mrežama. *CREST Certified Consultant* certifikat izdaje organizacija CREST koja je specijalizirana u izradi testera informacijske sigurnosti. CREST certifikat je time jedan od najboljih na području ispitivanja informacijske sigurnosti. CREST certificirane osobe mogu koristiti alate i tehnike za identificiranje ranjivosti u danom sustavu i one o tim ranjivostima konzultiraju osobu ili organizaciju koja je vlasnik sustava. CREST certificirane osobe sigurnosne probleme ne rješavaju, nego samo identificiraju. Prije dobivanja certifikata CREST, osoba mora imati CEH (eng. *Certified Ethical Hacker*) certifikat ili mora proći osnovni pismeni ispit. Tada se prelazi na praktični dio gdje je osoba dužna identificirati stvarne sigurnosne probleme i ranjivosti na nekom sustavu i tada ona postaje certificirana kao *CREST Certified Consultant.* Certifikat *CREST Certified Consultant* vrijedi 3 godine, a cijena certifikacije iznosi oko 320 $. Mogućnost certifikacije u Hrvatskoj još uvijek ne postoji. Više o certifikatu može se doznati na adresi:

http://www.crest-approved.org/

3.8. Cisco Career Certifications

Cisco Career Certifications su certifikacije specificirane za Cisco proizvode. Ispite za certificiranje provodi Pearson VUE (tvrtka za elektronička ispitivanja). Postoji 5 stupnjeva certifikacije: *entry, associate, professional, expert* i *architect*, kao i 7 različitih grana certifikacije: *routing & switching, design, network security, service provider, storage networking, voice* i *wireless*. U ovoj temi bitan je certifikat za mrežnu sigurnost punim imenom *Cisco Certified Network Professional-Security* (CCNP-*Security*) čiji je logo prikazan na slici 8. CCNP-*Security* certifikat je namijenjen Cisco inženjerima sigurnosti i on dokazuje znanja iz sigurnosti usmjeritelja, preklopnika te drugih mrežnih uređaja i programa, kao i znanja o odabiru, implementaciji i podršci u uspostavi vatrozidova (eng. *firewalls*) i virtualnih privatnih mreža (VPN). Ispit za certifikat CCNP-*Security* sastoji se od 65 pitanja od kojih je za prolaz potrebno točno odgovoriti na njih 55 u vremenu od 90 minuta. Svaki odgovor donosi jednak broj bodova i nema negativnih bodova. Mogućnost certificiranja u Hrvatskoj postoji i detalji su dani u nastavku dokumenta. Cisco certifikati traju 3 godine. Više informacija o CCNP-*Security* certifikatu, kao i o svim ostalim Cisco certifikatima može se naći na stranici u nastavku:

https://learningnetwork.cisco.com/index.jspa

Slika 8. Logo CCNP certifikata
Izvor: cisco.com

4. Organizacije koje dodjeljuju certifikate

4.1. (ISC)^2

(ISC)^2, ili punim imenom *International Information System Security Certification Consortium*, je globalna neprofitabilna organizacija osnovana 1989. godine koja se bavi edukacijom i certifikacijom stručnjaka iz područja informacijske sigurnosti. Sjedište (ISC)^2-a je na Floridi, SAD, a podružnice ima po svim razvijenijim zemljama i gradovima kao što su London, Hong Kong i Tokio. (ISC)^2 educira i certificira stručnjake u više od 135 zemalja diljem svijeta i time pokriva najveću površinu (nažalost, ne i Hrvatsku) od svih organizacija takvog tipa. Aktivnih stručnjaka s certifikatom organizacije (ISC)^2, po njihovom navodu, ima više od 30 tisuća i taj broj konstantno raste. Cilj (ISC)^2 certificiranja, kako sam (ISC)^2 navodi, je pružanje znanja i vještina iz područja informacijske sigurnosti u svrhu sigurnijeg društva te produktivnijeg i učinkovitijeg gospodarstva u svijetu. (ISC)^2 je razvio CBK (*Critical Body of Knowledge*), sažeti pregled svih bitnih tema iz informacijske sigurnosti. CBK definira globalne standarde informacijske sigurnosti koji su okosnica svih pravila i principa informacijske sigurnosti. U svrhu edukacije i certifikacije, (ISC)^2 nudi više vrsta certifikata. Osim gore navedenog CISSP (*Certified Information System Security Professional*) certifikata, nude se i sljedeći certifikati:

- *Systems Security Certified Practitioner* (SSCP): certifikat koji je primarno namijenjen stručnjacima kojima informacijska sigurnost nije osnovno zanimanje, ali se zahtjeva njezino poznavanje,
- *Certified Authorization Professional* (CAP): certifikat koji dokazuje znanja iz područja autorizacije i održavanja informacijskih sustava,
- *Certified Secure Software Lifecycle Professional* (CSSLP): certifikat koji osigurava znanja o sigurnosti tokom cijelog životnog ciklusa proizvoda u industriji,
- *Information Systems Security Architecture Professional* (CISSP-ISSAP): napredni CISSP certifikat sa specijalizacijom u arhitekturi informacijskih sustava,

- *Information Systems Security Engineering Professional* (CISSP-ISSEP): napredni CISSP certifikat sa specijalizacijom u inženjerstvu te
- *Information Systems Security Management Professional* (CISSP-ISSMP): napredni CISSP certifikat sa specijalizacijom u menadžmentu.

4.2. SANS Institute

SANS Institute (eng. *SysAdmin, Audit, Networking and Security*) je osnovan 1989. godine kao ogranak instituta *Escal Institute of Advanced Technologies* (EIAT). SANS institut se bavi edukacijom i certificiranjem iz područja informacijske sigurnosti. Osim certifikata, SANS omogućuje razne *online* treninge, prezentacije kao i seminare na mjesečnoj osnovi, sve na temu informacijske sigurnosti. SANS institut provodi brojne tečajeve iz područja informacijske sigurnosti te sigurnosti sustava i mreža, od kojih se većina provodi u tzv. virtualnim učionicama (SANS *vLIVE*), *online* treninzima i procjenama (SANS *OnDemand*) te treninzima uživo. Jedini certifikat SANS instituta je GIAC (*Global Information Assurance Certification*) i on predstavlja dokaz da su usvojena sva znanja koja SANS institut na svojim treninzima pruža. Posebnost SANS instituta je što je najviše orijentiran na sigurnost informacijskog sustava od svih nabrojanih organizacija.

4.3. EC-Council

EC-*Council* ili *International Council of E-Commerce Consultants* je organizacija osnovana 2006. godine koja certificira stručnjake iz područja e-poslovanja i informacijske sigurnosti. Svoje certifikate nude u preko 60 zemalja diljem svijeta i imaju više od 450 partnera u svijetu koji pod njihovom licencom educiraju i certificiraju stručnjake. Trening EC-*Councila* prošlo je preko 80 tisuća ljudi, dok njihov certifikat ima više od 30 tisuća osoba diljem svijeta. Od većih gradova njihove podružnice imaju Miami (sjedište), Dubai, Singapur, Kuala Lumpur, Mexico City i drugi. Cilj EC-*Councila*, kako oni navode, je pružiti besprijekornu sigurnost u informacijama i e-poslovanju svima kojima je ona potrebna. U tu svrhu, osim C|EH (*Certified Ethical Hacker*) certifikata, oni nude i sljedeće:

- *Computer Hacking Forensics Investigator* (CHFI): certifikat koji dokazuje znanja iz prepoznavanja hakerskih napada te općenito bilo kakvog računalnog kriminala,
- *License Penetration Tester* (LPT): certifikat kojim stručnjaci stječu znanja iz računalnih mreža te dopuštenog i nedopuštenog proboja u iste,
- *Certified Incident Handler* (C|IH): certifikat koji daje znanja iz područja uočavanja i sprečavanja sigurnosnih pogrešaka i anomalija u informatičkim sustavima,
- *Certified Secure Programmer* (C|SP): certifikat kojim se dokazuju znanja iz područja sigurnosti u razvoju programa,
- *Certified VoIP Professional* (ECVP): certifikat koji pruža znanja iz tehnologije VoIP (eng. *Voice over Internet Protocol*) i njene sigurnosti te
- *Network Security Administrator* (ENSA): certifikat koji dokazuje da je osoba stručnjak iz područja administriranja računalnih mreža.

4.4. CompTIA+

Organizacija *CompTIA+* (eng. *Computing Technology Industry Association*) je osnovana 1982. godine pod imenom *Association of Better Computer Dealers* (ABCD). *CompTIA+* se bavi edukacijom i certifikacijom stručnjaka iz područja informacijske tehnologije i industrije. Prema svojim navodima, *CompTIA+* je ukupno certificirala više od 80 tisuća ljudi diljem svijeta i to je čini jednom od najvećih organizacija za certifikaciju (uz Cisco) iz područja informacijske tehnologije u svijetu. *CompTIA+* se razgranala na više od 40 zemalja svijeta, a osim sjedišta u New Yorku ima poslovnice u gradovima kao što su London, Pariz te Sidney. Osim certifikata *Security+,* o kojem je već bilo riječi, *CompTIA+* izdaje i certifikate navedene u nastavku:

- *A+ certification:* za računalne tehničare,
- *Network+ certification:* za tehničare računalnih mreža,
- *Server+ certification:* za stručnjake u održavanju poslužitelja te operacijskih sustava,

- *CTT+ certification (Certified Technical Trainer): za* predavače na području informacijske tehnologije,
- *CDIA+ certification (Certified Document Imaging Architect):* za stručnjake u upravljanju dokumentima u informacijskoj tehnologiji,
- *Linux+ certification:* za stručnjake koji posjeduju specifična znanja operacijskih sustava *Linux* i *Unix*,
- *Project+ certification:* za stručnjake u upravljanju projektima,
- *RFID+ certification (Radio Frequency Identification):* za tehničare u korištenju tehnologija identifikacije radijskim frekvencijama te
- *PDI+ (Printing and Document Imaging):* za stručnjake koji imaju znanje potrebno za rad s pisačima, skenerima te *fax* i kopirnim uređajima.

4.5. ISACA

ISACA (*Information Systems Audit and Control Association*) je organizacija stručnjaka za reviziju, provjeru i sigurnost informacijskog sustava osnovana 1969. godine i to je čini najstarijom organizacijom tog tipa u svijetu. Danas ISACA broji više od 95 tisuća članova u svijetu i više od 200 lokalnih podružnica u skoro 160 zemalja. ISACA se bavi provjerom i nadgledanjem sustava u skoro svim poslovnim kategorijama, a neke od njih su bankarstvo i financije, računovodstvo, uprava te komunalne usluge. Osim provjerom i nadgledanjem, ISACA se bavi educiranjem i certificiranjem stručnjaka iz područja informacijske tehnologije. Četiri su certifikata koja ISACA izdaje, a osim već spomenutog CISM tu su i certifikati iz drugih disciplina informacijske tehnologije:

- *Certified Information Systems Auditor* (CISA): certifikat koji dokazuje da osoba ima znanja i vještine za upravljanje i nadgledanje informacijskog sustava,
- *Governance of Enterprise IT* (CGEIT): certifikat koji dokazuje da je osoba menadžer u informacijskoj tehnologiji, odnosno da je sposobna voditi ili upravljati IT tvrtkom ili sektorom tvrtke te
- *Risk and Information Systems Control certification* (CRISC): certifikat koji dokazuje da je osoba stručnjak u prepoznavanju rizika u informacijskoj tehnologiji i u razvijanju operacijskog sustava bez rizika.

4.6. ISECOM

ISECOM (*Institute for Security and Open Methodologies*) je zajednica posvećena informacijskoj sigurnosti osnovana 2001 godine. Osim standardnih poslova edukacije, certificiranja i izdavaštva kojim se manje više sve zajednice za informacijsku sigurnost bave, ono što je izdvaja je metodologija za ispitivanje ranjivosti sustava. Metodologija imena OSSTMM (eng. *Open Source Security Testing Methodology Manual*) nastala je zajedničkim radom svih prisutnih u zajednici te je za nju načinjen i jako praktičan priručnik koji se besplatno može skinuti s web stranica posvećenih toj metodologiji:

http://isecom.securenetltd.com/osstmm.en.2.1.pdf

Ukupan broj certificiranih osoba, po ISECOM-ovom navođenju, prelazi 50 tisuća. Osim certifikata OPST (OSSTMM Professional Security Tester), ISECOM izdaje još neke specijalizirane certifikate iz područja informacijske sigurnosti:

- *OSSTMM Wireless Security Expert* (OWSE): certifikat koji se dokazuje stručnost iz područja zaštite sigurnosti bežičnih mreža i informacija na njima,
- *Certified Trust Analyst* (CTA): certifikat kojim osoba dobiva znanja vođenja tvrtke ili sektora, donašenja odluka i upravljanja ljudskim potencijalima te
- *Hacker Highschool Teacher* (HHST): certifikat s kojim osoba može biti profesor tematike „*Hacker Highschool*“ (termin kojim se u SAD-u označava srednjoškolski program koji obuhvaća sigurnost operacijskih sustava i korištenja Interneta).

4.7. CREST

CREST ili *Council of Registered Ethical Security Testers* je organizacija koja se također bavi informacijskom sigurnošću, odnosno ispitivanjima sigurnosti informacijskih sustava i mreža. CREST je osnovan 1991. godine i do danas ima podružnice u više od 40 zemalja u svijetu. Središte mu je u New Yorku (SAD). CREST educira stručnjake o sigurnosnim problemima i anomalijama u sustavu. Osim edukacijom, CREST se bavi i certificiranjem stručnjaka na području ispitivanja informacijskih sustava. Jedini certifikat kojeg CREST izdaje je *CREST Certified Consultant,* no CREST surađuje s velikim brojem vanjskih partnera koji izdaju svoje certifikate, slične *Certified Consultantu* pod CREST-ovom licencom. Neki od poznatijih CREST-ovih partnera su *Commissum, BT Group, Ernst&Young, Global Secure Systems* te *Trustware*.

4.8. Cisco

Cisco je vodeća svjetska tvrtka u proizvodnji elektroničke, mrežne i telekomunikacijske opreme i rješenja. Osnovan je 1984. godine u San Franciscu. Središte firme je trenutno u San Joseu (Kalifornija). Cisco se bavi proizvodnjom sklopovlja kao što su usmjeritelji, preklopnici, modemi i slično, kao i programskih rješenja za svoje proizvode. Samim time što proizvode programska rješenja javila se potreba za zaštitom programa, sustava i mreža. Zbog te potrebe razvile su se razne Cisco akademije koje pružaju edukaciju i certifikate iz područja informacijske tehnologije kojom se Cisco bavi. Cisco navodi da za svaki certifikat koji on izdaje postoji između 20 i 30 tisuća certificiranih ljudi. U svijetu, ali i u Hrvatskoj, postoji veliki broj Cisco akademija, ali certifikati koje one izdaju se ne razlikuju jer ih sve licencira sam Cisco. Tako od certifikata, osim prije spomenutih certifikacija *CCNP-Security* vezanih uz informacijsku sigurnost, postoje i sljedeći certifikati vezani uz sigurnost:

- *Cisco Certified Network Professional* (CCNP): certifikat koji osobi daje dokaz da posjeduje znanja iz upravljanja računalnim mrežama srednje veličine (5-15 računala), uslugom QoS(eng. *Quality of Service)* te mrežama *VPN (eng. Virtual Private Network)* s naglaskom na informacijskoj sigurnosti,
- *Cisco Certified Design Professional* (CCDP): certifikat kojim se potvrđuje da osoba posjeduje relevantna znanja iz područja dizajna Ciscovih tehnologija,
- *Cisco Certified Internetwork Professional* (CCIP): certifikat koji dokazuje sposobnost stručnjaka na području mrežnih protokola koje Cisco koristi (*end-to-end, BGP* itd.),
- *Cisco Certified Voice Professional* (CCVP): certifikat koji pokriva znanja iz IP (eng. *Internet Protocol*) telefonije i VoIP mreža i programa,
- *Cisco Certified Network Professional Voice* (CCNP *Voice*): certifikat koji također obuhvaća znanja iz VoIP mreža i programa, ali s posebnim naglaskom na odabir optimalnih rješenja,
- *Cisco Certified Wireless Professional* (CCNP *Wireless*): certifikat koji daje potvrdu sposobnosti stručnjaka iz područja razvoja, administracije i nadgledanja bežičnih Cisco računalnih mreža.

5. Certifikati u Hrvatskoj

U Hrvatskoj se opisani certifikati iz područja informacijske sigurnosti mogu dobiti na više akademija. Ove akademije, osim certifikata iz područja informacijske sigurnosti, nude i neke druge certifikate koje licenciraju prije navedene organizacije. Neke od akademija na kojima se može steći znanje i certifikat iz informacijske sigurnosti, kao i vrste certifikata s okvirnom cijenom te web stranice s više informacija, navedene su u nastavku poglavlja.

- Učilište Algebra (slika 9) pruža mogućnost polaganja certifikata koje licenciraju EC-*Council*, CompTIA+ i Cisco. Certifikati iz područja informacijske sigurnosti koji se mogu steći na Učilištu Algebra su:
    - C|EH (*Certified Ethical Hacker*) – 15,928.50 kn – edukacija i certifikacijski ispit.
    - CompTIA *Security*+ – 12,632.00 kn – edukacija i certifikacijski ispit.
    - Cisco CCNP-*Security* – 4,920.00 kn – edukacija i certifikacijski ispit.

http://www.algebra.hr/Default.aspx

Slika 9. Logo Učilišta Algebra
Izvor: algebra.hr

- NetAkademija (slika 10) omogućuje polaganje certifikata kojeg licencira Cisco. Certifikat s okvirnom cijenom i adresa s više informacija su dani u nastavku:
    - Cisco CCNP-*Security* – 3,600.00 kn – edukacija i certifikacijski ispit.

http://netakademija.tvz.hr/cisco/ccna-security

Slika 10. Logo NetAkademije
Izvor: NetAkademija.tvz.hr

- CARNet (slika 11), kao i NetAkademija, omogućuje polaganje Cisco certifikata. CARNet također nudi pripremu za polaganje CompTIA Security+ certifikata. Certifikati s okvirnim cijenama dani su u nastavku teksta:
    - Cisco CCNP-Security – 3,500.00 kn – edukacija i certifikacijski ispit.
    - CompTIA Security+ - 6,200.00 kn – edukacija.

http://www.carnet.hr/camt/nastavni_program

Slika 11. Logo CARNet-a
Izvor: carnet.hr

- Edunet (slika 12) akademija je još jedna u nizu akademija koja pruža mogućnost Cisco edukacije i certifikacije. Certifikat kojeg Edunet nudi iz područja informacijske sigurnosti dan je u nastavku:
    - Cisco CCNP-Security – 3,600.00 kn

http://www.edunet.hr/ccnp/

Slika 12. Logo Edunet akademije
Izvor: edunet.hr

Polaganje certifikata kao što su CISSP, GIAC, *Security+*, CREST *Certified Consultant* i slični, za koje ne postoji certificiranje u Hrvatskoj, moguće je u bližem ili daljem inozemstvu. Prijavom za određeni certifikat sama organizacija koja ga dodjeljuje predlaže najbliže mjesto na kojem je moguće obaviti edukaciju i certifikaciju.

Certifikati iz područja informacijske sigurnosti koje izdaje neka hrvatska organizacija još ne postoje, ali uz razvitak informacijske tehnologije ovom brzinom i to bi se trebalo dogoditi u skoroj budućnosti.

6. Zaključak

Certifikat je službena potvrda da pojedinac ili organizacija posjeduje određena znanja i vještine. Često se koriste u računalnoj industriji za dokazivanje poznavanja određenih proizvoda i tehnologija. Certificirati se može osoba ili cijela organizacija. Ako se osoba želi certificirati, dužna je zadovoljiti određene preduvjete koje certifikat propisuje i položiti najčešće pismeni ispit kojim dokazuje znanja na području kojeg se certificira. Organizacija može dobiti certifikat ako je njezino poslovanje u skladu s normama po kojima je taj certifikat propisan. Na području informacijske sigurnosti organizacija može dobiti certifikat i taj certifikat dokazuje da je informacijska sigurnost organizacije u skladu s određenom normom. Certifikati iz područja informacijske sigurnosti koje osoba može dobiti pružaju znanja kao što su: etičko hakiranje, provjera pristupa, sigurnost sustava i mreže, ispitivanje informacijske sigurnosti i slično. Poznatiji certifikati iz područja informacijske sigurnosti su CISSP (*Certified Information System Security Professional),* GIAC *(Global Information Assurance Certification),* C|EH *(Certified Ethical Hacker),* CISM *(Certified Information Security Manager), Cisco Career Certifications* i slični. U Hrvatskoj se neki od tih certifikata mogu dobiti na licenciranim akademijama za edukaciju i certifikaciju, dok se za ostale moguće certificirati samo u inozemstvu. Akademija na kojoj se može dobiti najveći broj certifikata je Učilište Algebra, dok se Cisco certifikati mogu još dobiti i na Cisco akademijama kao što su NetAkademija, CARNet te Edunet. Nakon odluke o certificiranju potrebno je odrediti u kojim se područjima želi dokazati stručnost i prema tome odabrati certifikat. Edukacija za polaganje ispita za određene certifikate najčešće nije nužna, odnosno za ispite se pojedinac može samostalno pripremati pomoću *online* predavanja i vježbi koje se za svaki certifikat nude. Najveći problem je polaganje samog ispita jer se većina renomiranih certifikata ne može dobiti u Hrvatskoj. Budućnost bi trebala donijeti mogućnost polaganja svih poznatijih certifikata iz područja informacijske sigurnosti u Hrvatskoj. Neki trendovi predviđaju porast broja certifikata sa sve užim specijalizacijskim područjem, a time naravno i porast certificiranih stručnjaka u svijetu.

7. Reference

[1] (ISC)^2: CISSP® - Certified Information Systems Security Professional, https://www.isc2.org/cissp/default.aspx, srpanj 2010.

[2] GIAC: Information Security Certification for IT Security Professionals, http://www.giac.org/, rujan 2010.

[3] The CEH Program : Ethical Hacking and Countermeasurers, http://www.eccouncil.org/certification/certified_ethical_hacker.aspx, siječanj 2011.

[4] CompTIA+: CompTIA Security+, http://www.comptia.org/certifications/listed/security.aspx, lipanj 2010.

[5] ISACA: Certified Information Security Manager (CISM), http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager, lipanj 2010.

[6] ISECOM: OSSTMM Professional Security Tester Accredited Certification (OPST), http://www.isecom.org/projects/opst.shtml, travanj 2010.

[7] CREST: CREST Certified Consultant, http://www.crest-approved.org/CC, rujan 2010.

[8] Cisco: Cisco Networking Academy, http://www.cisco.com/web/learning/netacad/index.html, siječnj 2011.

[9] Algebra: Testiranje i certifikacija, http://www.algebra.hr/stranice/testiranje_i_certifikacija/ , lipanj 2010.

[10] NetAkademija: CCNP Certificiranje, http://netakademija.tvz.hr/certifikacijski-centar/vijesti/, prosinac 2010.

[11] Carnet: Certifikati, http://camt.carnet.hr/node/21, prosinac 2010.

[12] Edunet: Cisco certifikati, http://www.edunet.hr/cisco-certifikati/ studeni 2010.