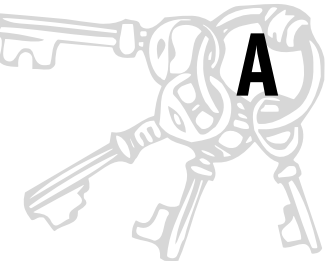


A

Sigurnosni standardi i programi sertifikacije

U ovom dodatku su ukratko pobrojani neki od sigurnosnih standarda i programa sertifikacije. Navedeni su neki međunarodni, a takođe i američki standardi i regulacioni propisi. Neki standardi opisani su u prethodnim poglavljima ove knjige a manji broj se prvi put pominje u ovom dodatku.

Programi sertifikacije vrlo su značajni u novije vreme jer omogućavaju određeni nivo standardizacije kvaliteta proizvoda i usluga, kao i kadrova koji rade u oblasti sigurnosti.

Kompletna lista važnih standarda zauzela bi verovatno polovinu ove knjige. Zato smo se odlučili da prikažemo samo mali broj reprezentativnih standarda, a ostale možete potražiti na Internetu ili kod organizacija za standardizaciju. Naveden je i postupak donošenja Internet standarda i RFC-ova, kao zanimljiv primer procesa *defacto* standardizacije koja je plod entuzijastičkog rada profesora i studenata, zatim inženjera i korisnika koji su razvijali prve TCP/IP mreže. Ovaj proces je kasnije formalizovan u okviru institucija, što će biti objašnjeno u ovom dodatku.

A.1 Sigurnosni standardi

ISO 17799

Standard ISO/IEC 17799 postavlja osnovne i opšte principe za iniciranje, implementaciju, održavanje i unapređenje upravljanja sigurnošću informacija u nekoj organizaciji. Pomenuti principi daju opšte smernice za zajednički prihvaćene ciljeve upravljanja sigurnošću informacija. ISO/IEC 17799:2005 se oslanja na najbolja iskustva upravljanja u sledećim područjima:

- sigurnosne polise
- organizacija sigurnosti informacija
- upravljanje vrednostima
- sigurnost ljudskih resursa
- fizička sigurnost i sigurnost okruženja
- upravljanje komunikacijama i operacijama
- kontrola pristupa
- akvizicija, razvoj i održavanje informacionih sistema
- rešavanje incidenata u oblasti sigurnosti
- upravljanje održanjem kontinuiteta posla
- poštovanje propisa i standarda

Preteča ovog standarda je Britanski standard BS7799-1.
Korisne adrese su:

- `http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=`
- `http://www.iso-17799.com/`
- `http://www.itgovernance.co.uk/page.bs7799`

ISO 27001

ISO/IEC 27001:2005 obuhvata sve vrste organizacija (komercijalna preduzeća, državne agencije, neprofitne organizacije). ISO/IEC 27001:2005 specificira zahteve za uspostavljanje, implementaciju, rad, nadzor, pregledanje, održavanje i unapređenje dokumentovanog sistema upravljanja sigurnošću kao delom poslovnih rizika te organizacije. Tu su specificirani zahtevi za implementaciju upravljanja sigurnošću za pojedinačne organizacije i njihove delove.

ISO/IEC 27001:2005 daje mogućnost izbora odgovarajućih sistema upravljanja za zaštitu imovine i stvaranja poverenja kod svih zainteresovanih strana. Primenjiv je na različite tipove i veličine kompanija, organizacija i institucija.

ISO/IEC 27001:2005 je pogodan za nekoliko različitih tipova primene, uključujući sledeće:

- korišćenje u organizacijama pri formulisanju sigurnosnih zahteva i ciljeva
- korišćenje u organizacijama, kao osiguranje da je upravljanje sigurnosnim rizicima efikasno
- korišćenje u organizacijama, kako bi se osiguralo poštovanje zakona i ostalih regulacionih propisa
- korišćenje u nekoj organizaciji, kao okvir procesa za implementaciju i rukovođenje kontrolom, kako bi pojedinačni sigurnosni ciljevi u toj organizaciji bili ispunjeni
- definisanje novih procesa u rukovođenju sigurnošću
- identifikacija i razjašnjenje postojećih procesa upravljanja sigurnošću informacija
- koristi ga rukovodstvo organizacija kako bi se odredio status aktivnosti koje se odnose na upravljanje sigurnošću informacija
- koriste ga interni i eksterni revizori (engl. *auditor*) organizacije kako bi se odredio stepen poštovanja polisa, direktiva i standarda koje je organizacija prihvatila
- koriste ga organizacije, kako bi poslovnim partnerima i drugim organizacijama s kojima sarađuju – ili iz komercijalnih razloga – obezbedile relevantne informacije o pravilima informacione sigurnosti, direktivama, standardima i procedurama
- implementacija informacione sigurnosti koja omogućava odvijanje posla
- koriste ga organizacije kako bi klijentima dostavile relevantne podatke o sigurnosti informacija.

Korisne adrese su:

- `http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103&ICS1=35&ICS2=40&ICS3=`
- `http://www.iso27001security.com/html/iso27000.html`

NIST standardi

Odeljenje za računarsku sigurnost američkog Nacionalnog instituta za standarde i tehnologiju (*National Institute of Standards and Technology*, NIST) uključeno je u mnogo različitih projekata. **CSRC** takođe obezbeđuje dosta resursa koji su raspoloživi *on-line*, a koji su zasnovani na ovim projketima.

Korisne adrese su:

- NIST Computer Security Division, Web stranica CSRC, `http://csrc.nist.gov/`
- NIST Computer Security Special Publications, `http://csrc.nist.gov/publications/nistpubs/`

Na primer, kriptografski algoritmi **DES** (Data Encryption Standard) i **AES** (Advanced Encryption Standard) jesu NIST standardi. O njima možete više pročitati u 3. poglavlju ove knjige i na sledećim Web stranicama:

- DES, `http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`
- AES, `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`

Zajednički kriterijum

Zajednički kriterijum (*Common Criteria*, CC) rezultat je napora da se naprave kriterijumi za proveru i vrednovanje IT sigurnosti koji će moći da se koriste u međunarodnoj zajednici. To je svojevrsno ujednačavanje velikog broja različitih izvornih kriterijuma: postojećih evropskih (ITSEC), američkih (TCSEC) i kanadskih kriterijuma (CTCPEC). Zajednički kriterijum razrešava konceptualne i tehničke razlike među izvornim kriterijumima. On i doprinosi razvoju međunarodnog standarda i otvara vrata ka uzajamnom priznavanju rezultata provere i vrednovanja.

Zajednički kriterijum je sada međunarodni standard (ISO/IEC 15408) za računarsku sigurnost. Za razliku od standarda kao što je USA standard FIPS 140, u CC-u se ne daje lista zahteva u pogledu sigurnosti ili funkcionalnosti koje proizvodi moraju da sadrže. Umesto toga, tu se opisuje radni okvir (engl. *framework*) u kome korisnici računarskih sistema i mreža mogu da specificiraju svoje zahteve; proizvođači (engl. *vendors*) mogu onda da ih implementiraju i/ili da iznesu stavove i tvrdnje o svojim proizvodima, a laboratorije mogu da provere i evaluiraju proizvode – da provere da li stvarno odgovaraju tim tvrdnjama, odnosno deklaracijama. Drugim rečima, CC obezbeđuje garanciju da će se proces specifikacije, implementacije i evaluacije proizvoda za računarsku sigurnost voditi i sprovesti na rigorozan i standardizovan način, što garantuje određeni nivo kvaliteta proizvoda i usluga u ovoj oblasti.

Korisne adrese su:

- `http://www.commoncriteriaportal.org/`
- `http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf`

Internet standardi i IETF

Poseban, vrlo značajan segment sigurnosti odnosi se na Internet. Mnogi su protokoli iz skupa protokola TCP/IP ili standardizovani ili su u procesu standardizacije. Internet ima sopstvene mehanizme standardizovanja, veoma različite od postupaka koji se primenjuju po standardima ITU-T i ISO. Prema univerzalnom dogovoru, organizacija poznata kao **Internet društvo** (engl. *Internet Society*) bavi se razvojem i publikovanjem ovih standarda. Tri organizacije pod okriljem Internet društva odgovorne su za stvarni rad na ovom području. To su:

- **Internet Architecture Board** (IAB), odgovorna za definiciju celokupne arhitekture Interneta; obezbeđuje rukovođenje, opšte principe i pravce razvoja za IETF. Kada je mreža ARPANET puštena u rad, Ministarstvo odbrane je obrazovalo formalni komitet da je nadgleda. Godine 1983. komitet je preimenovan u **Odbor za aktivnosti na Internetu** (engl. *Internet Activities Board*, IAB) i dodeljena mu je malo šira misija: podsticaće istraživače da mrežu razvijaju i održavaće Internet u približno istom duhu. Ista skraćenica (IAB) korišćena je i od onda kada je ime Odbora promenjeno u **Odbor za arhitekturu Interneta** (engl. *Internet Architecture Board*)[1].

  IAB se okuplja više puta godišnje da razmotri rezultate i da o njima izvesti organizacije koje su ga osnovale i koje ga finasiraju. Kada se ukaže potreba za novim standardom (na primer, za novim algoritmom za rutiranje), članovi IAB-a ga razmatraju, a zatim objavljuju izmene. Izmene su objavljivane u nizu tehničkih izveštaja zvanih **Zahtevi za komentare** (engl. *Request For Comments*, RFC). RFC dokumenti su skladišteni na mreži tako da ih svaki zainteresovani korisnik može preuzeti sa adrese `www.ietf.org/rfc`. Oni su numerisani hronološki, po redu pojavljivanja i danas ih ima preko 3.000. U ovoj knjizi se pozivamo na neke RFC dokumente.
- **Internet Engineering Task Force** (IETF), koja se bavi inženjeringom protokola i razvojem Inteneta. Do 1989. godine, Internet je tako narastao da opisani neformalni stil rada više nije bio primenljiv. Mnogi proizvođači su već nudili TCP/IP proizvode i nisu želeli da ih menjaju samo zato što šačica istraživača ima „bolju ideju". U leto 1989. godine, IAB je ponovo reorganizovan. Istraživači su prebačeni u **Istraživačke snage Interneta** (engl. *Internet Research Task Force*, *IRTF*) – telo podređeno IAB-u – i paralelno telo **Inženjerske snage Interneta** (engl. *Internet Engineering Task Force*, *IETF*). IAB su popunili predstavnici organizacija koje nisu više bile samo akademske i istraživačke. U početku je to bila grupa koja se sama obnavljala tako što su posle dvogodišnjeg mandata stari članovi imenovali nove. Kasnije je od osoba zainteresovanih za Internet obrazovano Internet društvo.

  Rad IETF-a je podeljen na osam područja, tj. na radne grupe: **opšte** (IETF procesi i procedure – na primer, proces za razvoj Internet standarda), **aplikacije ili primene** (protokoli zasnovani na Webu, EDI-Internet integracija, LDAP), **Internet infrastruktura** (IPv6, PPP proširenja), **operacije i upravljanje** (standardi i definicije za mrežne operacije, korišćenje i upravljanje – na primer SNMPv3 i daljinsko nadgledanje mreža), **rutiranje** (protokoli za rutiranje, kao što je OSPF), **sigurnost** (sigurnosni protokoli i tehnologije, kao što su Kerberos, IPSec, X.509, S/MIME, TLS), transport (protokoli transportnog nivoa, kao što su IP telefonija NFS, RSVP) i **korisničke usluge** (načini da se poboljša kvalitet informacija raspoloživih korisnicima Interneta; na primer, odgovorno

[1] http://www.iab.org/

korišćenje Interneta, korisničke usluge i dokumenti „vama za informaciju“ – engl. *for your information, FYI documents*).

Uočavamo da se oblast sigurnosti tretira kao posebno područje, što govori o značaju ove problematike u okviru Interneta.

- **Internet Engineering Steering Group** (IESG), odgovorna za tehničko upravljanje IETF aktivnostima i procesom donošenja Internet standarda.

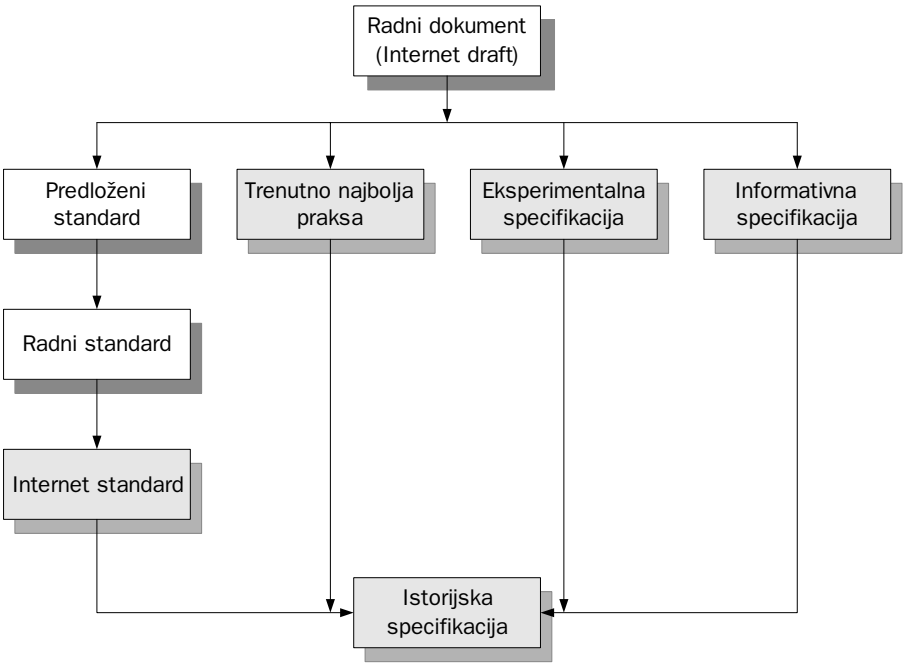
Odluku o tome koji će RFC postati Internet standard, donosi IESG, na predlog IETF-a. Da bi postala standard, specifikacija mora zadovoljiti sledeće kriterijume:

- da bude stabilna i razumljiva,
- da bude tehnički kompletna,
- da ono što specifikacija definiše ima više nezavisnih i interoperativnih implementacija koje su proverene u praksi,
- da ima značajnu javnu podršku,
- da bude prepoznatljiva i korisna u značajnom delu Interneta ili na celom Internetu.

Ključna razlika između ovih kriterijuma i onih koji se koriste kao internacionalni ITU standardi jeste isticanje radnog (operativnog) iskustva, odnosno primene u praksi.

Leva strana slike A.1 prikazuje niz koraka zvanih „standardna staza“ (engl. *standard track*), kojom prolazi specifikacija da bi postala standard. Ovaj proces je definisan u RFC 2026. Koraci podrazumevaju detaljno ispitivanje i testiranje. U svakom koraku, IETF može preporučiti unapređenje protokola i IESG mora da to ratifikuje. Proces počinje kada IESG odobri objavljivanje Internet nacrta (radnog dokumenta) kao RFC-a sa statusom „predloženi standard“ (engl. *Proposed Standard*).

Beli pravougaonici na dijagramu predstavljaju privremena stanja, u kojima se može biti minimalno vreme. Međutim, dokument mora ostati u fazi „predloženi standard“ najmanje 6 meseci i u fazi „nacrt standarda“ (engl. *Draft Standard*) najmanje 4 meseca kako bi bilo dovoljno vremena za pregled i recenziju dokumenta. Osenčeni pravougaonici predstavljaju dugoročna stanja u kojima se dokument može zadržati godinama. Da bi specifikacija postala nacrt standarda, moraju postojati najmanje dve nezavisne i interoperabilne implementacije iz kojih je dobijeno adekvatno operativno iskustvo. Kada se ostvari značajno implementaciono i operativno iskustvo, specifikacija se može podići na nivo Internet standarda. U ovoj tački, specifikacija dobija STD broj i RFC broj. Na kraju, specifikacija koja postane zastarela ili prevaziđena dobija istorijski status (engl. *historic*).



Slika A.1 *Internet RFC – proces publikovanja*

Svi Internet standardi spadaju u jednu od dve kategorije:

- Tehnička specifikacija (engl. *Technical specification*, TS). TS definiše protokol, uslugu, proceduru, konvenciju ili format. Gomila Internet standarda su TS-ovi.
- Izjava o primenljivosti (engl. *Applicability statement*, AS). AS specificira kako i pod kojim okolnostima jedan ili više TS-ova mogu biti primenjeni da podrže određenu Internet mogućnost (engl. *capability*).

Brojni RFC dokumenti ne postaju Internet standardi. U nekim RFC dokumentima standardizuju se rezultati dogovora, izjave o principima ili zaključci o tome koji je najbolji način da se izvrše određene operacije, kao i o IETF procesnim funkcijama. Takvi RFC dokumenti sadrže trenutno najbolju praksu (engl. *Best Current Practice*, BCP). Odobravanje BCP-ova odvija se isto kao i odobravanje predloženih standarda. Za razliku od dokumenata koji prolaze kroz sve etape na stazi standarda, nema trostepenog procesa za BCP; BCP prelazi iz stanja radnog dokumenta u odobreni BCP u jednom koraku.

Protokol ili druga specifikacija koja se ne smatra spremnom za standardizaciju, može se objaviti kao eksperimentalni RFC. Posle dodatnog rada, specifikacija može biti ponovo podneta na razmatranje. Ukoliko je specifikacija generalno stabilna, jasna i razumljiva, javno razmatrana i ocenjena povoljno, i ako za nju postoji dovoljan društveni interes i poverenje da bi se smatrala vrednom, RFC će postati predloženi standard.

Posle svega, Informativna specifikacij**a** (engl. *Informational Specification*) objavljuje se kao opšta informacija za Internet zajednicu.

PCI DSS (standard sigurnosti podataka industrije platnih kartica)

Kao odgovor na rastući broj zloupotreba (engl. *fraud*) u poslovanju na Internetu i – uopšte – u poslovanju kreditnim i sličnim karticama, nekoliko vodećih svetskih kompanija odlučile su da donesu sigurnosni standard koji bi pomogao da se smanje pronevere i zloupotrebe. Glavni inicijatori **PCI DSS** (*Payment Card Industry Data Security Standard*) standarda jesu Visa i Master Card International. Kasnije su ovaj standard prihvatile i ostale kompanije koje izdaju kreditne kartice. Doneti su i programi i definisane procedure sertifikacije kojima podležu kompanije koje se bave trgovinom preko Interneta uz primanje uplata kreditnim karticama. Kompanije koje prođu ovu sertifikaciju, imaju kod kompanija koje izdaju platne kartice značajno povoljnije uslove u pogledu provizija i načina refundiranja transakcija koje su posledica pronevera i zloupotreba. Ovaj standard obuhvata 12 područja svrstanih u 6 grupa. To su:

[I] Izgrađivanje i održavanje sigurne mreže

Zahtev 1: Instaliranje i održavanje konfiguracije zaštitne barijere radi zaštite podataka.

Zahtev 2: Ne koristiti podrazumevane vrednosti za lozinke i druge sigurnosne parametre.

[II] Zaštita podataka vlasnika platnih kartica

Zahtev 3: Zaštita uskladištenih podataka.

Zahtev 4: Šifrovanje podataka o karticama i drugih osetljivih informacija koje se prenose preko javnih mreža.

[III] Održavanje programa za rukovanje ranjivostima

Zahtev 5: Korišćenje i redovno ažuriranje antivirusnog softvera.

Zahtev 6: Razvoj i održavanje sigurnosnog sistema i aplikacija.

[IV] Implementacija strogih mera kontrole pristupa

Zahtev 7: Ograničavanje pristupa podacima po poslovnom principu „treba da zna“.

Zahtev 8: Dodela jedinstvene identifikacije svakom licu koje ima pristup računaru.

Zahtev 9: Ograničavanje fizičkog pristupa podacima o vlasnicima kartica.

[V] Redovno nadziranje i testiranje mreže

Zahtev 10: Praćenje i nadzor svih pristupa mrežnim resursima i podacima o vlasnicima kartica.

Zahtev 11: Redovno ispitivanje sigurnosnih sistema i procesa.

[VI] Održavanje politike sigurnosti informacija

Zahtev 12: Održavanje pravila koja se odnose na sigurnost informacija.

U trenutku pisanja ove knjige, PCI DSS standard je relativno nov i programi sertifikacije su tek u početnoj fazi. Korisna adresa je:

- `http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf`

A.2 Programi sertifikacije

Sigurnost je vrlo osetljivo područje. Mnoge firme i institucije žele da posebnu pažnju posvete proveri i sertifikaciji svojih proizvoda i usluga, kao i kadrova koji rade bilo kao zaposleni, bilo po ugovoru ili onih koji na drugi način (recimo kao poslovni partneri i saradnici) barataju osetljivim informacijama. Primera radi: u procesu ispitivanja mogu se otkriti osetljive informacije o organizaciji. Mnoge firme koje se bave ispitivanjem sigurnosti, trude se da dokažu kako ne zapošljavaju bivše hakere s crnim šeširima i kako se njihovi zaposleni na poslu drže strogih etičkih i moralnih principa.

Kao dodatna garancija pouzdanosti i poslovnosti ovih firmi, postoje sertifikati o stepenu poverenja, pouzdanosti i usklađenosti sa industrijskim standardima i najboljom praksom i procedurama, koje izdaju profesionalne i vladine (državne) institucije. U ovu svrhu su, pored standarda, uvedeni i brojni programi sertifikacija koje mogu propisivati vladine i zakonodavne agencije i/ili institucije, zatim profesionalne grupe i udruženja, a takođe i pojedini proizvođači opreme ili davaoci usluga. Navešćemo nekoliko predstavnika da bi čitaoci stekli osnovnu predstavu o njihovom domenu i obimu rada, kao i pristupu.

CISSP

Certified Information Systems Security Professional (CISSP®) sertifikacija daje profesionalcima u oblasti sigurnosti objektivno merilo kompetencije, kao i globalno priznat standard u pogledu dostignuća u ovoj oblasti. CISSP uverenje pokazuje kompetenciju u 10 domena (ISC) CISSP® CBK®. Ovo uverenje su akreditovale organizacije ANSI i ISO (ISO 17024:2003) u polju informacione sigurnosti.

CISSP uverenje, tj. sertifikat, potreban je rukovodiocima srednjeg i višeg nivoa koji nameravaju da budu ili su već na položajima CISO (Chief Information Security Officer), CSO (Chief Security Officer) ili Senior Security Engineer.

Korisne adrese su:

- CISSP Certification i (ISC)2 `https://www.isc2.org/`
- Web portal za sertifikovane profesionalce u oblasti računarske sigurnosti, `http://www.cissp.com/`

CHECK, CESG

U Velikoj Britaniji, glavni standard/akreditacija je CHECK šema koju administrira CESG (Communications-Electronics Security Group, deo GCHQ-a). Ovaj standard je obavezan preduslov za zapošljavanje u svim vladinim institucijama (centralnim, lokalnim, policijskim snagama itd.), i u mnogim komercijalnim „blue chip" organizacijama.[2] Organizacije potpisnici ove šeme dužne su da održavaju stroge etičke norme, a od nosilaca sertifikata se automatski zahteva da imaju najmanje SC nivo sigurnosne provere (engl. *SC level security clearance*).

GIAC

GIAC je skraćenica za Global Information Assurance Certification. GIAC je osnovan 1999. godine, kako bi se proveravale realne i praktične veštine profesionalaca u oblasti IT sigurnosti i izdavao sertifikat o tome. Sertifikat GIAC je svojevrsno jemstvo da ovlašćena osoba ima praktična znanja i veštine koje se mogu primeniti u ključnim oblastima računarske sigurnosti. GIAC trenutno nudi sertifikovanje za 18 specifičnih tipova poslovnih odgovornosti koje odražavaju tekuću praksu informacione sigurnosti. GIAC je jedinstven po tome što meri pojedine specifične oblasti znanja umesto opštih znanja u oblasti informatičke sigurnosti.

GIAC sertifikacije su klasifikovane u 5 osnovnih područja:

- Security Administration (administriranje sigurnosti)
- Management (menadžment)
- Operations (operacije)
- Legal (pravni aspekti)
- Audit (nadzor)

Postoji nekoliko nivoa sertifikacije: srebrna, zlatna i platinska (engl. *silver, gold, platinum*).

Korisna adresa je:

- `http://www.giac.org/`

Cisco Certified Security Professional (CCSP)

CCSP sertifikacija je potvrda posedovanja naprednih znanja i veština koje su potrebne da se Cisco mreže učine sigurnim. Profesionalac u oblasti računarskih mreža koji ima sertifikat CCSP, vlada veštinama potrebnim za upravljanje mrežnim infrastrukturama, zaštitu produktivnosti i smanjivanje troškova. U CCSP kurikulumu (engl. *curriculum*) naglašava se upravljanje VPN mrežama, Cisco Adaptive Security Device Manager (ASDM), PIX firewall, Adaptive Security Appliance (ASA), Intrusion Prevention Systems (IPS), Cisco Security Agent (CSA) kao i tehnike kojima se ove tehnologije kombinuju u jedinstvena i integrisana mrežna rešenja.

---

[2] Organizacije, odnosno kompanije koje su dobro organizovane, stabilne i nemaju veliki teret neizvršenih obaveza tj. dugovanja i zbog toga se ubrajaju u vrednije kompanije.

Korisna adresa je:

- `http://www.cisco.com/web/learning/le3/le2/le37/le54/learning_certification_type_home.html`

Information Systems Security (INFOSEC) Professional Recognition

Namena INFOSEC instrukcije je da ustanovi minimalni standard za obučavanje profesionalaca za sigurnost informacionih sistema (INFOSEC) i to u oblasti telekomunikacija i automatizovanih informacionih sistema.

Američka direktiva *National Security Telecommunications and Information Systems Security Directive* No. 501 sadrži zahtev da sva federalna ministarstva i agencije sprovedu programe obuke za INFOSEC profesionalce. Kao što je definisano u NSTISSD 501, INFOSEC profesionalac je osoba koja je odgovorna za pregled/nadzor ili rukovođenje, ili za nacionalne sigurnosne sisteme tokom određenih faza životnog ciklusa. Direktiva 501 implementira se kroz zajednički rad odeljenja i agencija koje su obavezne da zadovolje INFOSEC obrazovne zahteve na najbolji i najefikasniji način. Ova instrukcija je prva u seriji standarda koji definišu minimum obuke i obrazovanja; ona treba da pomognu ministarstvima i agencijama da postignu i zadovolje zahteve u ovim područjima. Instrukcija važi kako za njihove zaposlene, tako i za saradnike po ugovoru (engl. *contractors*).

Korisne adrese:

- `http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf`
- `http://niatec.info/pdf/4011.pdf`