# CompTIA Security+: SY0-601 Vodič za sertifikaciju

*Prevod drugog izdanja*

**U potpunosti obuhvata nov CompTIA Security+ (SY0-601) ispit i pomaže vam da ga položite iz prvog pokušaja.**

**Ian Neil**

kompjuter biblioteka

Packt›

**Izdavač:**

kompjuter biblioteka

Obalskih radnika 4a, Beograd

**Tel: 011/2520272**

**e-mail:** kombib@gmail.com

**internet:** www.kombib.rs

**Urednik:** Mihailo J. Šolajić

**Za izdavača, direktor:**
Mihailo J. Šolajić

**Autor:** Ian Neil

**Prevod:** Slavica Prudkov

**Lektura:** Nemanja Lukić

**Slog:** Zvonko Aleksić

**Znak Kompjuter biblioteke:**
Miloš Milosavljević

**Štampa:** „Pekograf“, Zemun

**Tiraž:** 500

**Godina izdanja:** 2022.

**Broj knjige:** 549

**Izdanje:** Prvo

**ISBN:** 978-86-7310-572-7

# CompTIA Security+: SY0-601 Certification Guide Second Edition



ISBN 978-1-80056-424-4

# O AUTORU

**Ian Neil** je jedan od najboljih svetskih predavača za Security+. On je u stanju da razdvoji informacije u delove kojima se lako upravlja, tako da ljudi bez prethodnog znanja steknu veštine potrebne za dobijanje sertifikata. Nedavno je radio za američku vojsku u Evropi i dizajnirao kurs Security+ sa izuzetno uspešnom stopom prolaznosti, koji je služio ljudima iz svih oblasti (ne samo IT profesionalcima). On je MCT, MCSE, A+, Network+, Security+, CASP i RESILIA praktičar, koji je u protekle 23 godine radio sa vrhunskim provajderima obuke i bio jedan od prvih tehničkih predavača koji je obučavao interno osoblje Microsoft-a kada su otvorili svoju kancelariju u Bukureštu 2006. godine.

# O RECENZENTIMA

**Crystal Voiles** je IT stručnjak sa više od 30 godina iskustva u IT oblasti, od operatera za tehničku podršku, preko podrške za desktop računare, do sistemske administracije i podrške za sajber bezbednost.

Poslednjih 10 godina radila je kao stručnjak za sajber bezbednost i upravljala sa nekoliko alata za sajber bezbednost, uključujući **Assured Compliance Assessment Solution**(**ACAS**), **Host-Based Security System**(**HBSS**), Tanium, **System Center Configuration Manager**(**SCCM**) i **Enterprise Mission Assurance Support Service** (**eMASS**).

Trenutno radi kao **Menadžer bezbednosti informacionih sistema** (**ISSM**) za malu medicinsku organizaciju odgovornu za koordinaciju i sprovođenje bezbednosnih politika i kontrole, kao i za procenu ranjivosti unutar medicinske kompanije. Ona je odgovorna za obradu podataka i bezbednost mreže, upravljanje bezbednosnim sistemima i istragu kršenja bezbednosti. Ona upravlja rezervnim i sigurnosnim sistemima, obukom zaposlenih za približno 900 naloga krajnjih korisnika, merama bezbednosnog planiranja i oporavkom podataka u situacijama testiranja katastrofe.

Njeni sertifikati obuhvataju **Certified Information Systems Security Professionals** (**CISSP**), **CompTIA Advanced Security Practitioner** (**CASP**+), Security +, **Microsoft CertifiedProfessional** (**MCP**), SCCM i ITIL Foundations.

**Rebecca Moffitt** je iskusan konsultant za bezbednost informacija i rizike, sa 8 godina iskustva u industriji.

Rebeka se pridružila QA-u u oktobru 2018. godine i od tada radi kao stručnjak u sajberbezbednosti. Njene oblasti su prvenstveno vezane za sajberbezbednost, bezbednost informacija, osiguravanje informacija i upravljanje rizikom. Ona je ne-

davno stekla CISM putem ISACA-e, a CSRM putem PECB-a. Ona je sertifikovana Information Security Management Systems Lead Implementer i dobro poznaje ISO27001, 27002, 27005 i standarde ISO 31000, 27035 i 19011, kao i razne radne okvire za sajber, informacije i rizik.

Rebeka je strastvena u pogledu svoje profesije i posvetila je vreme radu sa mlađim generacijama, podizanju njihove svesti o oblasti sajber/informacione bezbednosti i izazivanju njihovog entuzijazam za potencijalnu karijeru u sajber bezbednosti.

Rebeka je Kanađanka. Seoski način života joj je ukorenjen. Ona voli sve stvari vezane za život na istočnoj obali: žurke u kuhinji, kantri muziku i povrće.

*Želela bih da zahvalim svojoj porodici, na neprestanoj ljubavi i podršci.*

*- Rebeka Mofit*

**Sunil Gupta** je iskusan kompjuterski programer i stručnjak za sajber bezbednost i konsultant je za informacione tehnologije sa fokusom na sajber bezbednost. On je priznat govornik i član mnogih ključnih organizacija.

Sunil je pomogao mnogim organizacijama širom sveta, uključujući Barclays Banku; Aviation College Qatar (QATAR); Ethiopian Airlines; Telecom Authority Tanzania; NCB banka (Saudijska Arabija); Accenture (Indija); Afghan Wireless (Avganistan); i još mnogim drugim.

Trenutno onlajn obučava više od 60.000 studenata, iz više od 170 zemalja, a neka od njegovih najboljih dela objavile su velike izdavačke kuće. Neki od njegovih najboljih kurseva su: End-to-End Penetration Testing with Kali Linux i Threat and Vulnerability Assessment for Enterprises.

Njegovi sertifikati za sajber bezbednost obuhvataju **SSCP sertifikat** (**Systems Security Certified Practitioner**), **Bug Bounty Program Certification**, kao i mnoge druge.

# PACKT TRAŽI AUTORE POPUT VAS

Ako ste zainteresovani da postanete autor za Packt, posetite authors.packtpub.com i prijavite se danas. Radili smo sa hiljadama programera i tehnoloških profesionalaca, baš kao što ste i vi, da bismo im pomogli da podele svoj uvid sa globalnom tehnološkom zajednicom. Možete da izvršite osnovnu prijavu, da se prijavite za određenu popularnu temu za koju tražimo autora, ili da pošaljete neku svoju ideju.

# Kratak sadržaj

# Sadržaj

## POGLAVLJE 7

## DEO III



## POGLAVLJE 9



## POGLAVLJE 10

# Predgovor

Ova knjiga će vam pomoći da razumete osnove bezbednosti, od CIA trijade do upravljanja identitetom i pristupom. U ovoj knjizi opisujemo mrežnu infrastrukturu i kako se ona razvija implementacijom virtuelizacije i različitih cloud modela i njihovo skladištenje. Naučićete kako da obezbedite uređaje i aplikacije koje kompanija koristi.

## Kome je namenjena ova knjiga

Ova knjiga je dizajnirana za svakoga ko želi da položi CompTIA Security+ SY0-601ispit. Ona je odskočna daska za svakoga ko želi da postane profesionalac za bezbednost ili da pređe u oblast sajber bezbednosti.

## Šta obuhvata ova knjiga

*Poglavlje 1*, *Razumevanje osnova bezbednosti* - obuhvata neke osnove bezbednosti koje će biti detaljnije opisane u narednim poglavljima.

*Poglavlje 2*, *Implementacija infrastrukture javnog ključa* - opisujemo različite tipove enkripcije i načine izdavanja i korišćenja sertifikata.

*Poglavlje 3*, *Provera identiteta i upravljanje pristupom* - razmatramo različite tipove autentifikacije. Opisujemo koncepte upravljanja identitetom i pristupom.

*Poglavlje 4*, *Istraživanje virtuelizacije i koncepata cloud-a* - upoznajemo vas sa raznim cloud modelima i sa cloud bezbednošću, posmatranjem njihovog okruženja za raspoređivanje i skladištenje.

*Poglavlje 5*, *Monitoring, skeniranje i penetracioni testovi* - opisujemo penetracione testove, tipove vežbi, skeniranje, lov na pretnje i SIEM sisteme.

*Poglavlje 6*, *Sigurni i nesigurni protokoli* - opisujemo kada se koriste određeni sigurni protokoli.

*Poglavlje 7*, *Mreža i bezbednosni koncepti* - opisujemo mrežne komponente, daljinski pristup i alate za izviđanje mreže.

*Poglavlje 8*, *Bezbednost bežičnih i mobilnih rešenja* - razmatramo bežična rešenja i bezbedna mobilna rešenja.

*Poglavlje 9*, *Identifikacija pretnji, napada i ranjivosti*– istražujemo napade i ranjivosti, analizirajući redom svaki tip napada i identifikujući njegove jedinstvene karakteristike. Ovo poglavlje je verovatno najbolje testiran modul na Security+ ispitu.

*Poglavlje 10*, *Upravljanje, rizik i saglasnost* - razmatramo upravljanje rizikom i propise, kao i radne okvire.

*Poglavlje 11*, *Upravljanje bezbednošću aplikacija* - razmatramo razvoj aplikacija i bezbednost.

*Poglavlje 12*, *Procedure za odgovor na incident*– obuhvata pripremu za oporavak od katastrofe i metode oporavka u praksi.

*Poglavlje 13*, *Test 1* - sadrži pitanja, zajedno sa objašnjenjima, koja će vam pomoći da procenite da li ste spremni za test.

*Poglavlje 14*, *Test 2* – sadrži još više pitanja, zajedno sa objašnjenjima, koja će vam pomoći da procenite da li ste spremni za test.

# Da biste izvukli maksimum iz ove knjige

U ovom vodiču za sertifikaciju pretpostavljamo da nemate prethodno znanje o proizvodu. Potrebno je da u potpunosti razumete informacije da biste postali sertifikovani.

# Dodatni onlajn resursi

Dalju podršku za ispite i dodatne resurse za vežbu možete da nađete na veb sajtu autora, na adresi `www.securityplus.training`. Dodatni materijali sadrže uputstva za ispite, kartice za učenje, pitanja zasnovana na performansama i probne ispite.

# Preuzmite slike u boji

Takođe imate na raspolagannju PDF fajl koji sadrži kolorne slike ekrana/dijagrama upotrebljene u ovoj knjizi. Fajl možete da preuzmete na adresi:

https://bit.ly/3rmB2xJ

# Korišćene konvencije

U ovoj knjizi se koristi niz konvencija.

`Kod u tekstu`: Označava kodne reči u tekstu, nazive tabela baza podataka, nazive direktorijuma, nazive fajlova, ekstenzije fajlova, nazive putanja, lažne URL adrese, korisnički unos i Twitter postove. Evo primera: „Problem koji se javlja je taj da `strcpy` ne može da ograniči veličinu karaktera koji su kopirani.“

Blok koda je postavljen na sledeći način:

```
int fun (char data [256]) {
int I
char tmp [64], strcpy (tmp, data);
}
```

Svaki unos ili izlaz komandne linije je napisan na sledeći način:

```
Set-ExecutionPolicy Restricted
```

**Podebljan ispis**: Označava novi termin, važnu reč ili reči koje vidite na ekranu. Na primer, reči u menijima ili okvirima za dijalog prikazuju se tako u tekstu. Evo primera:„**SSID** je i dalje omogućen. Administrator bi trebalo da označi polje pored opcije **Disable Broadcast SSID**.“

Saveti su prikazani ovako.

Važne napomene su prikazani ovako.

# Stupite u kontakt

Povratne informacije naših čitalaca su uvek dobrodošle.

**Opšte povratne informacije**: Ako imate pitanja o bilo kom aspektu ove knjige, u naslovu vaše poruke istaknite naslov knjige i pošaljite nam e-mail na kombib@gmail.com

Štamparske greške: Iako smo se potrudili da obezbedimo tačnost našeg sadržaja, greške se dešavaju. Ako ste pronašli grešku u ovoj knjizi, bili bismo vam zahvalni ako biste nam to prijavili. Molimo posetite stranicu knjige https://bit.ly/3tl0Z2W i ostavite komentar.

**Piraterija**: Ako na internetu naiđete na nelegalne kopije naših radova u bilo kom obliku, bili bismo vam zahvalni ako biste nam dali adresu ili naziv veb sajta. Kontaktirajte nas na `kombib@gmail.com` i pošaljite link do sumnjivog materijala.

# Ciljevi CompTIA Security+601 ispita

U nastavku su navedeni ciljevi ispita za CompTIA 601 sertifikat i relevantna poglavlja u knjizi u kojima se nalaze informacije. Postoji sveobuhvatan indeks koji će vam pomoći da pronađete određenu ispitnu temu. Dodatne resurse za ispit možete naći na adresi: `www.securityplus.training`.

Detalji ispita su sledeći:

- Šifra ispita: SY0-601
- Broj pitanja: Maksimalno 90
- Vrste pitanja: višestruki izbor i pitanja zasnovana na performansama
- Trajanje: 90 minuta

# Ciljevi ispita (domeni)

Sledeće tabele pokazuju poglavlja u kojima su obuhvaćeni različiti definisani domeni mereni ispitivanjem:

| DOMEN | PROCENAT ISPITA |
|---|---|
| 1.0 - Napadi, pretnje, ranjivosti | 24% |
| 2.0 - Arhitektura i dizajn | 21% |
| 3.0 – Implementacija | 25% |
| 4.0 - Operacije i odgovor na incident | 16% |
| 5.0 - Upravljanje, rizik i saglasnost | 14% |
| Ukupno | 100% |

| 1.0 - NAPADI, PRETNJE I RANJIVOSTI | | |
|---|---|---|
| **BROJ** | **OPIS** | **POGLAVLJE** |
| 1.1 | Poređenje i razlikovanje različitih tehnika društvenog inženjeringa | 9 |
| 1.2 | Analiza potencijalnih indikatora tipa napada, sa obzirom na dati scenario | 9 |
| 1.3 | Analiza potencijalnih indikatora povezanih sa napadima aplikacije, sa obzirom na dati scenario | 9 |
| 1.4 | Analiza potencijalnih indikatora povezanih sa mrežnim napadima, sa obzirom na dati scenario | 8, 9 |

| 1.0 - NAPADI, PRETNJE I RANJIVOSTI | | |
|---|---|---|
| 1.5 | Objašnjenje različitih vrsta pretnji, vektora i izvora inteligencije | 9, 10, 11 |
| 1.6 | Objašnjenje bezbednosnih briga povezanih sa različitim tipovima ranjivosti | 9, 10 |
| 1.7 | Rezime tehnika upotrebljenih za procenu bezbednosti | 5, 6, 9 |
| 1.8 | Objašnjenje tehnika u penetracionim testovima | 5 |

| 2.0 - ARHITEKTURA I DIZAJN | | |
|---|---|---|
| **BROJ** | **OPIS** | **POGLAVLJE** |
| 2.1 | Objašnjenje važnosti bezbednosnih koncepata u okruženju preduzeća | 1, 2, 8, 11, 12 |
| 2.2 | Rezime koncepata virtuelizacije i cloud računarstva | 4 |
| 2.3 | Rezime razvoja i raspoređivanja sigurne aplikacije i koncepata automatizacije | 11 |
| 2.4 | Rezime koncepata dizajna autentifikacije i autorizacije | 3 |
| 2.5 | Implementiranje otpornosti sajber bezbednosti sa obzirom na dati scenario | 7, 12 |
| 2.6 | Objašnjenje bezbednosnih implikacija ugrađenih i specijalizovanih sistema | 11 |
| 2.7 | Objašnjenje važnosti kontrole fizičke bezbednosti | 1 |
| 2.8 | Rezimiranje osnova kriptografskih koncepata | 2 |

| 3.0 – IMPLEMENTACIJA | | |
|---|---|---|
| **BROJ** | **OPIS** | **POGLAVLJE** |
| 3.1 | Implementacija sigurnih protokola sa obzirom na dati scenario | 6 |
| 3.2 | Implementacija bezbednosnih rešenja hosta ili aplikacije sa obzirom na dati scenario | 7, 11 |
| 3.3 | Implementacija sigurnog mrežnog dizajna sa obzirom na dati scenario | 6, 7 |
| 3.4 | Instaliranje i konfigurisanje bezbednosnih podešavanja bežične mreže sa obzirom na dati scenario | 3, 8 |
| 3.5 | Implementiranje sigurnih mobilnih rešenja sa obzirom na dati scenario | 8 |
| 3.6 | Primena rešenja sajber bezbednosti na cloud sa obzirom na dati scenario | 4 |
| 3.7 | Implementacija kontrola za upravljanje identitetom i nalogom sa obzirom na dati scenario | 3 |
| 3.8 | Implementacija rešenja za autentifikaciju i autorizaciju sa obzirom na dati scenario | 3, 6 |
| 3.9 | Implementiranje infrastrukture javnog ključa sa obzirom na dati scenario | 2 |

| 4.0 - OPERACIJE I ODGOVOR NA INCIDENT | | |
|---|---|---|
| **BROJ** | **OPIS** | **POGLAVLJE** |
| 4.1 | Upotreba odgovarajućeg alata za procenu organizacione bezbednosti sa obzirom na dati scenario | 7 |
| 4.2 | Rezime važnosti pravila, procesa i procedura za odgovor na incident | 12 |
| 4.3 | Primena odgovarajućih izvora podataka za podršku istraživanju sa obzirom na dati incident | 5, 7, 12 |
| 4.4 | Primena tehnika, ili kontrola za ublažavanje, za obezbeđivanje okruženja sa obzirom na dati incident | 5, 7 |
| 4.5 | Objašnjenje ključnih aspekata digitalne forenzike | 1 |

| 5.0 - UPRAVLJANJE, RIZIK I SAGLASNOST | | |
|---|---|---|
| **BROJ** | **OPIS** | **POGLAVLJE** |
| 5.1 | Poređenje i razlikovanje različitih tipova kontrola | 1 |
| 5.2 | Objašnjenje važnosti primenjivih propisa, standarda ili radnih okvira koji utiču na stav organizacione bezbednosti | 10 |
| 5.3 | Objašnjenje važnosti pravila za organizacionu bezbednost | 3, 10 |
| 5.4 | Rezime procesa i koncepata upravljanja rizikom | 10 |
| 5.5 | Objašnjenje koncepata privatnosti i poverljivih podataka u odnosu na bezbednost | 10 |


# Postanite član Kompjuter biblioteke

Kupovinom jedne naše knjige stekli ste pravo da postanete član Kompjuter biblioteke. Kao član možete da kupujete knjige u pretplati sa 40% popustai učestvujete u akcijama kada ostvarujete popuste na sva naša izdanja. Potrebno je samo da se prijavite preko formulara na našem sajtu. Link za prijavu: http://bit.ly/2TxekSa


Skenirajte QR kod
registrujte knjigu
i osvojite nagradu

# DEO I

## Svrha i ciljevi bezbednosti

U ovom delu ćete učiti o osnovama bezbednosti, od CIA trijade do identifikacije i upravljanja pristupom.

Ovaj deo se sastoji od sledećih poglavlja:

- **Poglavlje 1,** Razumevanje osnova bezbednosti
- **Poglavlje 2**, Implementacija infrastrukture javnog ključa
- **Poglavlje 3**, Provera identiteta i upravljanje pristupom
- **Poglavlje 4**, Istraživanje virtuelizacije i koncepata cloud-a

# 1

# Razumevanje osnova bezbednosti

U ovom poglavlju ćemo opisati neke osnove bezbednosti koje će vam pomoći da identifikujete i ublažite bezbednosne pretnje u sistemu. S obzirom na to da je sajber kriminal u porastu iz dana u dan, kao profesionalac **Informacione tehnologije** (**IT**) neophodno je da prvo razumete ove osnovne koncepte.

Ovim poglavljem obuhvaćene su sledeće teme:

- Osnove bezbednosti
- Poređenje tipova kontrole
- Fizičke kontrole bezbednosti
- Razumevanje digitalne forenzike

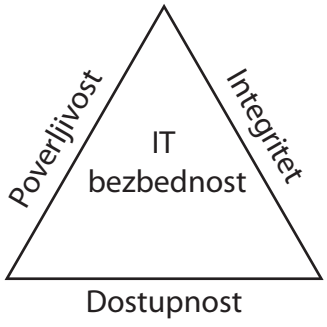
Počnimo pregledom osnova bezbednosti.

# Osnove bezbednosti

Osnove bezbednosti su osnova zaštite naše imovine i mora da postoji strategija ili metodologija koju prilagođavamo za bezbednost. To je CIA trijada, koju ćemo sada analizirati.

## IA koncept

Većina knjiga o bezbednosti počinje osnovama bezbednosti, predstavljanjem CIA trijade - to je konceptualni model dizajniran da pomogne onima koji pišu propise za bezbednost informacija u okviru organizacije. To je široko korišćen bezbednosni model i predstavlja poverljivost, integritet i dostupnost, tri ključna principa koje bi trebalo da koristite da biste garantovali da imate siguran sistem:




**Slika 1.1** – CIA trijada

Detaljnije ćemo opisati ove principe:

- **Poverljivost**: Sprečava otkrivanje podataka neovlašćenim osobama tako da samo ovlašćene osobe imaju pristup podacima. To je poznato kao osnova koju je potrebno znati. Pristup bi trebalo da imaju samo oni koji bi trebalo da znaju sadržaj. Na primer, vaša medicinska istorija dostupna je samo vašem lekaru i nikome drugom.

  Takođe, imamo tendenciju da vršimo enkripciju podataka da bi oni ostali poverljivi. Postoje dve vrste enkripcije, poznate kao simetrična i asimetrična. Simetrična enkripcija koristi jedan ključ, poznat kao tajni ključ. Asimetrična enkripcija koristi dva ključa, poznata kao privatni ključ i javni ključ.

- **Integritet**: To znači da znate da podaci nisu menjani ili da njima nije manipulisano. Koristimo tehniku pod nazivom heširanje koja koristi podatke i konvertuje ih u numeričku vrednost koju nazivamo heš ili sažetak poruke. Kada sumnjate da je došlo do promena, proverava se heš vrednost u odnosu na original. Ako se heš vrednost promenila, onda su podaci promenjeni. Uobičajeni algoritmi heširanja obuhvaćeni ispitom su **Secure Hash Algorithm Version 1** (**SHA1**) 160-bitni i **Message Digest Version 5** (**MD5**) 128-bitni. SHA1 je sigurniji od MD5; međutim, MD5 je brži. Što je veći broj bitova, to je algoritam sigurniji, a što je broj bitova manji, to je brži.
- **Dostupnost**: Dostupnost osigurava da su podaci uvek dostupni; na primer kada želite da kupite avionsku kartu, a sistem se vraća sa greškom koja govori da ne možete da je kupite. To bi moglo da bude frustrirajuće i stoga je dostupnost važna. Primeri dostupnosti uključuju **Redundant Array of Independent Disks**(**RAID**), koji omogućava da se jedan ili dva diska prekinu, dok su podaci i dalje dostupni. Drugi primer može da bude klaster preklapanja. U ovom slučaju, dva servera mogu da pristupe istim podacima, a ako jedan ne uspe, drugi i dalje može da obezbedi podatke, rezervnu kopiju podataka ili **Heating Ventilation Air Conditioning**(**HVAC**) koji reguliše temperaturu za važne servere. U data centru, ako je temperatura previsoka, serveri će se isključiti.

## Najniža privilegija

**Najniža privilegija** je mesto gde nekome dajete samo najograničeniji pristup koji je potreban da bi mogao da obavlja svoju poslovnu ulogu; to je poznato kao osnova koju je *potrebno znati*. Kompanija će napisati propis najniže privilegije tako da administratori znaju kako da njome upravljaju.

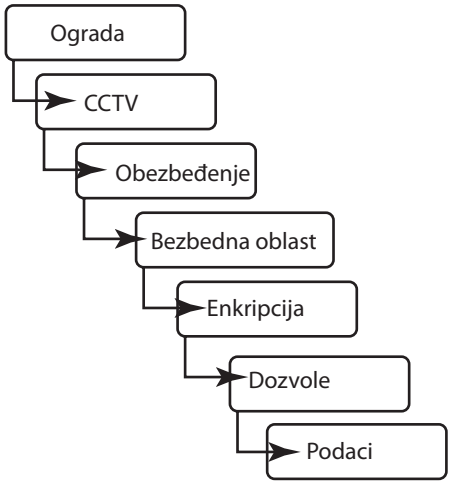
## Detaljan model odbrane

**Detaljna odbrana** je koncept zaštite podataka kompanije nizom zaštitnih slojeva, tako da ako je jedan sloj neuspešan, drugi sloj će već biti na mestu da spreči napad. Počinjemo primer podacima koje ćemo zatim da šifrujemo da bismo ih zaštitili:

- Podaci se čuvaju na serveru.
- Podaci imaju dozvole za fajlove.
- Podaci su šifrovani.

- Podaci se nalaze u bezbednom delu zgrade.
- Na ulazu u zgradu nalazi se obezbeđenje koje proverava identifikaciju.
- Postoji CCTV oko perimetra.
- Oko perimetra je visoka ograda.

Pogledajmo ovo iz perspektive uljeza koji pokušava da preskoči ogradu da vidimo koliko slojeva mora da zaobiđe:




**Slika 1.2** – Detaljan model odbrane

Sada ćemo uporediti različite tipove kontrole.

# Poređenje načina kontrole

Postoji širok izbor različitih bezbednosnih kontrola koje koristimo za ublažavanje rizika od napada; tri glavne kategorije su upravljačka, operaciona i tehnička kontrola. Pogledaćemo ih detaljnije; potrebno je da budete upoznati sa svakom od ovih kontrola i da znate kada je svaku od njih potrebno da primenite. Počnimo tako što ćemo pogledati tri glavne kontrole.

## Upravljačke kontrole

**Upravljačke kontrole** pišu menadžeri da bi kreirali organizacione propise i procedure za smanjenje rizika unutar kompanija. Oni uključuju regulatorne radne okvire tako da kompanije budu u skladu sa zakonima. Slede primeri upravljačkih kontrola:

- **Godišnja procena rizika**: Kompanija će imati registar rizika gde će finansijski direktor posmatrati sve rizike povezane sa novcem, a IT menadžer će posmatrati sve rizike koje predstavlja IT infrastruktura. Kako se tehnologija menja i hakeri postaju sofisticiraniji, rizici mogu da postanu veći. Svako odeljenje će identifikovati svoje rizike i tretmane rizika i postaviti ih u registar rizika, koje bi trebalo pregledati na godišnjem nivou.
- **Penetracioni testovi/skeniranje ranjivosti**: Skeniranje ranjivosti nije nametljivo jer samo proverava ranjivosti, dok je penetracioni test nametljiviji, jer ide dublje u računar i može da iskoristi ranjivosti. To može da dovede do neočekivanog pada sistema. To će biti dalje objašnjeno kasnije u ovoj knjizi.

## Operacione kontrole

Operacione kontrole sprovode zaposleni u kompaniji tokom svog svakodnevnog poslovanja. Primeri ovih kontrola su sledeći:

- **Godišnja obuka za podizanje svesti o bezbednosti**: To je godišnji događaj na kom se podsećate šta bi trebalo da radite svaki dan da biste zaštitili kompaniju:

  *Primer 1* – Kada završite dnevne obaveze, trebalo bi da očistite svoj sto i da zaključate sve dokumente.

  *Primer 2* – Zaposleni i posetioci bi trebalo u svakom trenutku da nose identifikacione bedževe. Ako to ne rade, trebalo bi ih opomenuti.

  *Primer 3* – Kompanijama je potrebno da njihovi zaposleni završe godišnju obuku sajber bezbednosti jer je rizik svakim danom sve veći.

- **Upravljanje promenama**: To je proces koji kompanija usvaja da promene koje su napravljene ne bi izazvale bezbednosne rizike za kompaniju. Promena jednog odeljenja mogla bi da utiče na drugo odeljenje. **Change Advisory Board** (**CAB**) pomaže u određivanju prioriteta promena; oni takođe gledaju na finansijske koristi od promene i mogu da prihvate ili da odbiju predložene promene u korist kompanije. IT se brzo razvija i naši

procesi će morati da se promene da bi se nosili sa potencijalnim bezbednosnim rizicima povezanim sa novijom tehnologijom.

- **Plan kontinuiteta poslovanja**: To je planiranje postupanja u nepredviđenim situacijama da bi se poslovanje održalo i kada dođe do katastrofe, tako što bi se identifikovala svaka pojedinačna tačka kvara koja sprečava rad kompanije.

## Tehničke kontrole

**Tehničke kontrole** su one koje implementira IT tim da bi se smanjio rizik za poslovanje.

Ove kontrole mogu da uključuju sledeće:

- **Firewall pravila**: Firewall-ovi sprečavaju neovlašćen pristup mreži putem IP adrese, aplikacije ili protokola. Oni su detaljnije obrađeni kasnije u ovoj knjizi.
- **Antivirus/antimalver**: To je najčešća pretnja za poslovanje i moramo da obezbedimo da svi serveri i desktop računari budu zaštićeni i ažurirani.
- Čuvari ekrana: Isključuju računare kada su neaktivni, sprečavajući pristup.
- **Filteri ekrana**: Sprečava ljude koji prolaze da čitaju podatke na vašem ekranu.
- **Intrusion Prevention System (IPS) / Intrusion Detection System (IDS)**: IDS nadgleda mrežu da otkrije bilo kakve promene, a IPS zaustavlja napade. Ako nemate IDS, IPS takođe može da ispuni ulogu IDS-a. Oni su detaljnije obrađeni u *poglavlju 7*.

Pogledajmo sada druge tipove kontrole, od udaljavajućih do fizičkih kontrola, kada pokušavamo da zaustavimo napade na izvoru.

## Udaljavajuće kontrole

**Udaljavajuće kontrole** mogu da budu CCTV i senzori pokreta. Kada neko prolazi pored zgrade i senzori pokreta ga detektuju, pale se svetla da bi ga udaljila od zgrade. Zgrada sa CCTV kamerom na istaknutom mestu i znakom koji upozorava ljude da ih snimaju može da deluje kao odvraćanje.

## Istraživačke kontrole

**Istraživačke kontrole** služe za istragu incidenta koji se dogodio i koji je potrebno istražiti; to bi moglo da obuhvata sledeće:

- **CCTV** beleži događaje dok se odigravaju pa možete da vidite ko je bio u određenoj prostoriji ili ušao kroz prozor na zadnjoj strani zgrade. CCTV može da snimi kretanje i da obezbedi dokaze.
- **Fajlovi evidencije** su tekstualni fajlovi koji beleže događaje i vreme kada su se desili; mogu da beleže trendove i obrasce tokom određenog vremenskog perioda. Na primer, serveri, desktop računari i firewall-ovi imaju evidencije događaja koje detaljno opisuju radnje koje se dešavaju. Kada saznate vreme i datum događaja, možete da prikupite informacije iz različitih fajlova evidencije. Oni mogu biti sačuvani u **Write-Once Read-Many** (**WORM**) diskovima tako da ih možete čitati, ali ne i menjati.

## Ispravljačke kontrole

**Ispravljačke kontrole** su radnje koje preduzimate za oporavak od incidenta. Možete da izgubite hard disk koji sadrži podatke; u tom slučaju biste zamenili podatke iz rezervne kopije koju ste prethodno napravili.

**Sistemi za suzbijanje požara** su još jedan oblik ispravljačke kontrole. Možda je došlo do požara u vašem centru podataka koji je uništio mnoge servere, stoga, kada kupite zamenske servere, možete da instalirate sistem za suzbijanje kiseonika koji će vatri uskratiti potreban kiseonik. Ovaj metod koristi argon/azot i ugljen-dioksid da istisne kiseonik iz serverske sobe.

## Kontrole nadoknade

**Kontrolu nadoknade** takođe možemo da nazivamo**Alternativna** ili **Sekundarna kontrola** i možemo da je koristimo umesto primarne kontrole, koja je bila neuspešna ili nije dostupna. Kada je primarna kontrola neuspešna, potrebna nam je sekundarna kontrola. To je slično kao kada idete u kupovinu i imate 100 dolara u gotovini - kada potrošite gotovinu, moraćete da koristite kreditnu karticu kao kontrolu nadoknade.

*Primer*: Kada dođe novi zaposlenik, trebalo bi da se prijavi pomoću pametne kartice i PIN koda. Za dobijanje nove pametne kartice može biti potrebno 3–5 dana, tako da se tokom perioda čekanja zaposleni može prijavljivati korišćenjem korisničkog imena i lozinke.

## Preventivne kontrole

**Preventivne kontrole** postoje da odvrate svaki napad; na primer, to može da bude čuvar koji sa velikim psom šeta oko zgrade. To bi nateralo nekoga ko pokušava da provali da dobro razmisli o tome. Neke od preventivnih mera koje mogu da se preduzmu su sledeće:

- **Onemogućavanje korisničkih naloga**: Kada neko napusti kompaniju, prvo što se dešava je da mu se nalog onemogući, jer ne želimo da izgubimo informacije kojima ima pristup, a zatim je potrebno da promenimo lozinku da mu se onemogući pristup. Takođe možemo da onemogućimo nalog dok su ljudi na privremenom radu, porodiljskom odsustvu, ili ako otkrijemo da je taj nalog korišćen u napadu na našu mrežu.
- **Učvršćivanje operativnog sistema**: To čini računar sigurnijim, pri čemu obezbeđujemo da je operativni sistem potpuno zakrpljen i isključujemo nekorišćene funkcije i servise. To će osigurati da ne postoji ranjivost. Ministarstvo odbrane SAD (DOD) ima vodič pod nazivom Security Technical Implementation Guide (STIG), koji sadrži uputstva o tome kako da „zaključate" računarske sisteme i softver da biste sprečili da budu ranjivi na napade.

## Pristupne kontrole

Tri glavna dela pristupne kontrole su identifikacija pojedinca, njegova autentifikacija kada unese lozinku ili PIN, a zatim autorizacija, gde se pojedincu daje dozvola za različite nivoe podataka. Na primer, nekome ko radi u finansijama biće potreban viši nivo bezbednosne provere jer pristupa drugačijim podacima od osobe koja šalje porudžbinu gotove robe:

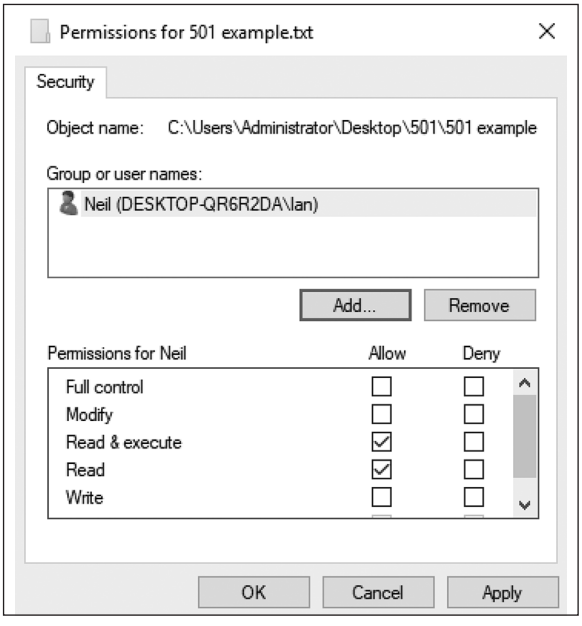
- **Identifikacija**: To je slično kao da svako ima svoj bankovni račun; račun se identifikuje prema detaljima računa na bankovnoj kartici. Identifikacija u bezbednom okruženju može da podrazumeva posedovanje korisničkog naloga, pametne kartice ili možda neke vrste biometrijskih podataka, kao što su otisak prsta ili lice jer su jedinstveni za svakog pojedinca. Svaka osoba ima svoj **bezbednosni identifikator** (**SID**) za nalog, što je kao serijski broj naloga.
- **Autentifikacija**: Kada pojedinac unese svoj metod identifikacije, zatim mora da bude autentifikovan, na primer, unosom lozinke ili PIN-a.
- **Autorizacija**: To je nivo pristupa ili dozvola koje morate da primenite na izabrane podatke. Obično ste član određenih grupa, na primer, menadžer prodaje može da pristupi podacima iz grupe za prodaju, a zatim da pristupi podacima iz grupe menadžera. Dobićete samo minimalnu količinu pristupa koji je potreban za obavljanje vašeg posla; to je poznato kao najniža privilegija.

## Diskreciona pristupna kontrola

**Diskreciona pristupna kontrola** je slična **New Technology File System** (**NTFS**) dozvolama za fajlove, koje se koriste u Microsoft operativnim sistemima. Korisniku se daje pristup koji mu je potreban za obavljanje posla. Ponekad ih nazivamo kontrolom zasnovanom na korisniku ili usredsređenom na korisnika. Dozvole su sledeće:

- **Full Control**: Potpun pristup.
- **Modify**: Menjanje podataka, čitanje i čitanje i izvršenje.
- **Read and Execute**: Čitanje fajla i pokretanje programa ako se nalazi unutar njega.
- **List Folder Contents**: Proširenje direktorijuma da biste videli poddirektorijume unutar njega.
- **Read**: Čitanje sadržaja.
- **Write**: Omogućava da pišete u fajl.
- **Special Permissions**: Omogućava detaljan pristup; na primer, razdvaja svaku od prethodnih dozvola na detaljniji nivo.
- **Data Creator/Owner**: Osobu koja kreira neklasifikovane podatke zovemo vlasnik i on je odgovoran za proveru ko ima pristup tim podacima.

Na dijagramu prikazan je korisnik *Ian* koji ima dozvole **Read** i **Read & Execute**:




**Slika 1.3** – Dozvole za DAC fajlove

# Obavezna pristupna kontrola

**Obavezna pristupna kontrola** (**MAC**) zasniva se na nivou klasifikacije podataka. MAC procenjuje kolika bi šteta mogla biti naneta interesima nacije. One su sledeće:

- **Top secret**: Najviši nivo, izuzetno teško oštećenje
- **Secret**: Dovodi do ozbiljne štete
- **Confidental**: Dovodi do štete
- **Restricted**: Neželjeni efekti

Primeri MAC-a na osnovu nivoa klasifikacije podataka su sledeći:

- **Top secret**: Projekat nuklearne energije
- **Secret**: Istraživanje i razvoj
- **Confidential**: Tekuća pravna pitanja

## MAC uloge

Nakon što su poverljivi podaci napisani, oni su u vlasništvu kompanije. Na primer, ako pukovnik napiše poverljiv dokument, on pripada vojsci. Pogledajmo tri uloge:

- **Owner**: To je osoba koja piše podatke i ona je jedina osoba koja može da odredi klasifikaciju. Na primer, ako pišu tajni dokument, oni će ga postaviti na tom nivou, ne na višem.
- **Steward**: To je osoba odgovorna za kvalitet i obeležavanje podataka.
- **Custodian**: Čuvar je osoba koja čuva i upravlja poverljivim podacima. Čuvar obezbeđuje da su podaci šifrovani i da je kreirana rezervna kopija.
- **Security Administrator**: Administrator bezbednosti je osoba koja daje pristup poverljivim podacima nakon što je dato odobrenje.

# Pristupna kontrola na bazi uloga

Pristupna kontrola zasnovana na ulogama je podskup odeljenja koji obavlja podskup zadataka unutar odeljenja. Na primer, dve osobe u odeljenju za finansije koje rukuju samo sitnim novcem. U pogledu IT-a, to bi mogle da budu dve osobe u IT timu koje administriraju server e-pošte.

## Pristupna kontrola na bazi pravila

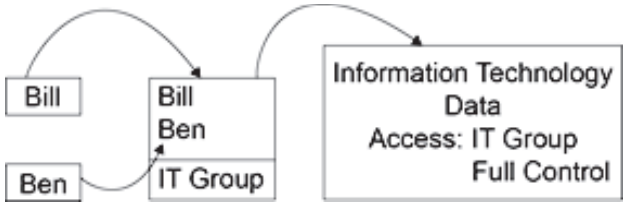
U **pristupnoj kontroli zasnovanoj na pravilima (Rule-Based Access Control -RBAC**), pravilo se primenjuje na sve ljude u odeljenju, na primer, izvođači će imati pristup samo između 8 i 17 časova, a ljudi iz službe za pomoć će moći da pristupe samo zgradi 1, gde je njihovo radno mesto . Ova kontrola može da bude vremenski zasnovana ili da ima neku vrstu ograničenja, ali se odnosi na celo odeljenje.

## Pristupna kontrola na bazi atributa

U **pristupnoj kontroli zasnovanoj na atributu (Attribute-Based Access Control - ABAC**), pristup je ograničen na osnovu atributa u nalogu. Džon bi mogao da bude izvršni direktor i neki podaci bi mogli da budu ograničeni samo na one sa atributom izvršni. To je korisnički atribut iz usluga imenika, kao što je odeljenje ili lokacija. Možda ćete želeti da date različite nivoe kontrole različitim odeljenjima.

## Pristupna kontrola na bazi grupe

Da bi se kontrolisao pristup podacima, ljudi mogu da se svrstaju u grupe da bi se pojednostavio pristup. Na primer, dve osobe koje rade u IT-u kojima je potreban pristup IT podacima. Na primer, nazovimo ih *Bill* i *Ben*. Prvo ćemo ih postaviti u IT grupu, a zatim toj grupi dajemo pristup podacima:




**Slika 1.4** – Pristup na bazi grupe

Drugi primer je kad članovi prodajnog tima mogu da imaju potpunu kontrolu nad podacima o prodaji korišćenjem pristupa zasnovanog na grupi, ali će vam možda biti potrebna dva nova početnika koji imaju pristup samo za čitanje. U tom slučaju, potrebno je da kreirate grupu pod nazivom novi početnici i da ljudima unutar te grupe date dozvolu samo za čitanje podataka.

## Pristupna kontrola na bazi Linux-a

U ovom odeljku ćemo opisati dozvole za Linux fajlove. Oni se često pojavljuju na Security+ ispitu, iako nisu obuhvaćeni ciljevima ispita.

## Dozvole za Linux fajlove (ne SELinux)

Dozvole za Linux fajlove su u numeričkom formatu; **prvi broj** predstavlja **vlasnika**, **drugi broj** predstavlja **grupu**, a **treći broj** predstavlja **sve ostale** korisnike:

**a.** Dozvole:

- **Vlasnik**: Prvi broj
- **Grupa**: Drugi broj
- **Svi ostali korisnici**: Treći broj

**b.** Numeričke vrednosti:

- **4**: Čitanje
- **2**: Pisanje
- **1**: Izvršenje

Za razliku od Windows dozvole koja će izvršiti aplikaciju, funkcija izvršenja u Linux-u vam omogućava da pregledate ili pretražujete. Dozvola 6 bi bila dozvola za čitanje i pisanje. Vrednost 2 bi bila dozvola za pisanje, a vrednost 7 bi bila dozvola za čitanje, pisanje i izvršenje. Slede primeri:

- *Primer 1*: Ako imam *764* pristup za *File A*, to bi moglo da se raščlani na sledeći način:
  **a. Vlasnik**: Čitanje, pisanje i izvršenje
  **b. Grupa**: Čitanje i pisanje
  **c. Svi ostali korisnici**: Čitanje

Drugi način na koji dozvole mogu da se postave je po abecednim vrednostima, na sledeći način:

**a. R:** Čitanje
**b. W**: Pisanje
**c. X**: Izvršenje

Kada koristite abecedne vrednosti, svaki skup dozvola je prikazan kao tri crtice. Potpuna kontrola za tri entiteta je sledeća:

**a. Vlasnik puna kontrola**: `rwx --- ---`
**b. Grupna puna kontrola**: `--- rwx ---`
**c. Svi ostali korisnici - puna kontrola**: `--- --- rwx`

- *Primer 2*: Ako fajl ima nivo pristupa `rwx rwx rw-`, šta to znači?
  - **a.** Vlasnik ima dozvolu za čitanje, pisanje i izvršenje (potpuna kontrola).
  - **b.** Grupa ima dozvolu za čitanje, pisanje i izvršenje (potpuna kontrola).
  - **c.** Svi ostali korisnici imaju dozvole samo za čitanje i pisanje.

# Fizička bezbednosna kontrola

Fizičke bezbednosne kontrole se postavljaju da bi se sprečio neovlašćen pristup kompaniji ili pristup podacima. Fizičke bezbednosne kontrole je lako identifikovati, jer možete da ih dodirnete. Pogledajmo svaku od njih redom.

## Opsežna bezbednost

U ovom odeljku ćemo opisati različite tipove opsežnih sigurnosnih sistema:

- **Oznake i natpisi**: Pre nego što bilo ko dođe do glavnog ulaza, trebalo bi da postoje dobro vidljivi znakovi koji ga upozoravaju da ulazi u obezbeđeno područje, sa naoružanim čuvarima i psima. To se koristi kao sredstvo odvraćanja da bi se sprečili mogući uljezi.
- **Ograde/Kapije**: Prva linija odbrane bi trebalo da bude perimetarska ograda, jer otvorenost mnogih lokacija čini ih veoma ranjivim na uljeze. Pristup lokaciji može da se kontroliše korišćenjem kapije kojom upravlja obezbeđenje ili čitač rastojanja. Možete da postavite stubove ispred zgrade da sprečite automobil da prođe kroz ulaz. Možda čak imate različite zone, kao što je odeljenje za istraživanje i razvoj, koje ima sopstveno obezbeđenje perimetra.
- **Kontrola pristupa**: Naoružani stražari na kapiji bi trebalo da provere identitet onih koji ulaze. Trebalo bi da postoji lista kontrole pristupa za posetioce koje sponzoriše interno odeljenje. Čuvari koji proveravaju identitet trebalo bi da budu iza jednosmernog kaljenog stakla tako da posetioci ne mogu da vide unutrašnjost stražarnice.
- **Predvorja za kontrolu pristupa**: Neko ko ulazi u zgradu otvara jedna vrata u prostor (predvorje za kontrolu pristupa) u kom obezbeđenje može da potvrdi njegov identitet pre nego što mu dozvoli ulazak u prostorije kroz druga vrata.
- **Evidencija posetilaca**: Čuvari na glavnom ulazu u bazu ili kompaniju će tražiti od posetilaca da popune evidenciju posetilaca, a zatim da daju neki dokument za identifikaciju.

- **Značke**: Forma identifikacije se zadržava, a dodeljuje im se bedž posetioca koji je različite boje od boje značke zaposlenih. Kada odlaze, vraćaju bedž i vraća im se obrazac za identifikaciju. Ove značke bi trebalo da budu vidljive u svakom trenutku, a trebalo bi zatražiti značku od svakoga kome nije istaknuta. Značke za članove osoblja mogu da budu kartice sa omogućenim RFID-om, tako da mogu da pristupe zgradi korišćenjem čitača kartica.
- **Osvetljenje**: Osvetljenje se postavlja iz dva glavna razloga: prvi razlog je da može da se vidi svako ko pokuša da uđe na vašu lokaciju noću, a drugi razlog je bezbednost.
- **Kamere**: Kamere mogu biti postavljene u oblastima oko perimetra i na vratima za detektovanje pokreta. Mogu biti podešene da detektuju objekte i danju i noću da bi alarmirale bezbednosni tim.
- **Robotizovani stražari**: Mogu biti podešeni da patroliraju perimetrom i da uzvikuju upozorenja da bi odvratili uljeze. Ti stražari patroliraju DMZ-om između Severne i Južne Koreje i mogu da budu naoružani:

**Slika 1.5** – Robot stražar

Zamke, ograde i okretnice su sve fizičke kontrole koje mogu da zaustave uljeze.

- **Industrijska kamuflaža**: Kada pokušavate da zaštitite područje visoke bezbednosti, projektujte zgradu tako da bude zaštićena od snimaka iz vazduha, tako što će izgledati kao stambeni objekti. Zamaskirajte i ulaze. To će otežati operativcima nadzora da je uoče.

## Građevinska bezbednost

U ovom odeljku ćemo opisati različite tipove sigurnosnih sistema za zgrade:

- **Stražari**: Oni rade na recepciji, na ulazu, da bi proveravali lične karte ljudi koji ulaze u zgradu i da bi sprečili neovlašćen pristup. Ti čuvari bi trebalo da budu naoružani, a jedan od čuvara bi trebalo da bude sa psom. Postupali bi prema pravilima kontrole pristupa da bi se osiguralo da se neovlašćenom osoblju uskrati pristup.
- **Integritet/kontrola dve osobe**: To povećava nivo bezbednosti na ulazu u zgradu jer obezbeđuje da je neko dostupan za rad sa posetiocima čak i kada druga osoba razgovara telefonom. To bi takođe smanjilo rizik od zlonamernog insajderskog napada.
- **Upravljanje ključem**: Ovde se ključevi odeljenja svakodnevno odjavljuju i prijavljuju da bi se sprečilo da neko uzme ključeve i napravi njihove kopije.
- **Zamke**: To su okretni uređaji koji dozvoljavaju prolaz samo jednoj osobi. One održavaju bezbedno okruženje, uglavnom za centar podataka. Centar podataka ima mnogo servera za različite kompanije.
- **Blizinske kartice**: To su beskontaktni uređaji gde se pametna kartica postavlja u blizinu uređaja za blizinsku karticu da bi se dobio pristup vratima ili zgradi.
- **Tokeni**: Tokeni su mali fizički uređaji na kojima dodirujete blizinsku karticu da biste ušli u ograničeno područje zgrade. Neki tokeni vam omogućavaju da otvorite i zaključate vrata pritiskom na sredinu samog tokena; drugi prikazuju kod nekoliko sekundi pre nego što istekne.
- **Biometrijske brave**: Biometrija je jedinstvena za svaku osobu; primeri su korišćenje otiska prsta, mrežnjače, dlana, glasa, skener zenice ili prepoznavanja lica.
- **Elektronske brave**: Korišćenjem elektronske brave, više vam nije potreban ključ za pristup zgradi; potreban vam je samo PIN. Možeteda ih podesite tako da se ne otvaraju, da se otvore tokom nestanka struje, ili da budu bezbedne, odnosno da vrata ostaju zaključana.
- **Protivprovalni alarmi**: Postavljaju se kada se prostorije ne koriste, pa kada neko pokuša da provali u vaše prostorije, to će aktivirati alarm i obavestiti nadzornu kompaniju ili lokalnu policiju.
- **Protivpožarni alarmi / detektori dima**: U zgradi preduzeća, u svaku prostoriju se postavljaju protivpožarni alarmi ili detektori dima, pa kada izbije požar i alarmi se aktiviraju, ljudima unutar prostorija je omogućeno da pobegnu.

- **Unutrašnja zaštita**: Možete da imate sigurne oblasti i bezbedan ograđen prostor; prvi primer bi bio kontejner od kaljenog stakla ili čvrste mreže, oba sa bravama za ograničenje pristupa. Takođe možete da imate zaštićenu distribuciju za kablove, što izgleda kao metalni stub unutar kog se nalaze mrežni kablovi. Filteri ekrana koji se koriste na desktopu mogu da spreče nekoga da čita sa ekrana.
- **Provodnici**: Provodnici ili kablovska distribucija imaju postavljene kablove. To štiti kablove od manipulisanja, a sprečava i da ih glodari pregrizu.

Provodnici i kablovska distribucija štite Ethernet kabl između zidne utičnice, kroz zgradu sve do patch panela.

- **Kontrole životne sredine**: HVAC i sistemi za gašenje požara su takođe bezbednosna kontrola. U centru podataka ili serverskoj prostoriji temperatura mora da bude niska, jer će se u suprotnom serveri pregrejati i otkazati. Tu se koristi tehnika koju zovemo topli i hladni prolazi za regulisanje temperature.

## Zaštita uređaja

U ovom odeljku ćemo opisati različite sisteme zaštite uređaja:

- **Kablovske brave**: One su priključene na laptopove ili tablete da bi se osiguralo da niko ne može da ih ukrade.
- **Vazdušni zazor**: Računar je isključen sa mreže i nema kablovsku ili bežičnu vezu da bi se osiguralo da podaci ne budu ukradeni. Primer za to je računar u odeljenju za istraživanje i razvoj, jer želimo da sprečimo pristup njemu preko mrežnog kabla. Jedini način da ubacite ili uklonite podatke iz mašine sa vazdušnim zazorom je korišćenje prenosivih medija kao što je USB drajv.

Vazdušni zazor je izolovani računar; jedini način za izdvajanje podataka je korišćenje USB ili CD ROM-a.

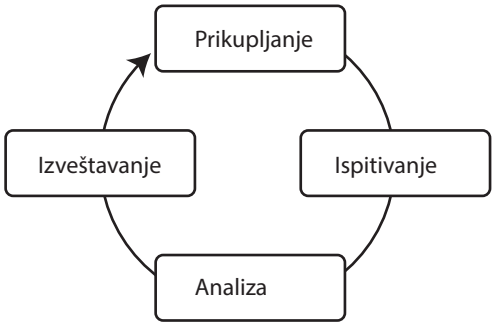
- **Sef za laptop**: Laptopovi i tableti su skupi, ali podaci koji se na njima nalaze mogu da budu neprocenjivi, stoga postoje sefovi za skladištenje laptopova i tableta.

- **USB blokator podataka**: Ovaj uređaj blokira pinove za podatke na USB uređaju, što sprečava hakera da izvrši krađu kada punite svoj USB uređaj na javnom mestu.
- **Trezor**: Ovde podaci mogu biti šifrovani i čuvani u cloud-u, što vam daje izuzetno bezbedno skladište. Možete da koristite trezor lozinki na svom računaru da biste zaštitili sve svoje lozinke, ali on je siguran samo onoliko koliko ga štiti glavna lozinka.
- **Faradejev kavez**: To je metalna konstrukcija, poput metalne mreže koja se koristi za smeštaj pilića. Kavez sprečava bežične ili mobilne telefone da rade unutar kompanije. To bi moglo da bude ugrađeno u strukturu prostorije koja se koristi kao sigurno područje. Takođe sprečava da bilo koja vrsta emisije napusti kompaniju.

# Razumevanje digitalne forenzike

Policija koristi digitalnu forenziku kada istražuje zločine i treba da pronađe digitalne dokaze da bi obezbedila osudu. Govorićemo o kompjuterskim napadima i napadima na mreži.

Godine 2006. Forensic Process 19, koji je predložio NIST, sastojao se od četiri faze: prikupljanje, ispitivanje, analiza i izveštavanje. Sledi dijagram koji prikazuje te faze:




**Slika 1.6** – Forenzički ciklus

Pogledajmo svaku od ovih faza:

- **Prikupljanje**: Ovde se podaci ispituju, zatim izdvajaju sa medija na kom se nalaze, a zatim se konvertuju u format koji može da se ispita pomoću forenzičkih alata.
- **Ispitivanje**: Pre ispitivanja, podaci će biti heširani, a zatim će se izvršiti istraga relevantnim forenzičkim alatom. Kada se ispitivanje završi, podaci

se još jednom heširaju da bi se osiguralo da ih ispitivač ili alati nisu menjali.

- **Analiza**: Kada se prikupe svi forenzički podaci, oni se analiziraju i zatim transformišu u informacije koje mogu da budu upotrebljene kao dokaz.
- **Izveštavanje**: Sastavlja se izveštaj koji može da se koristi kao dokaz za osuđujuću presudu.

Postoji mnogo različitih komponenti forenzičke istrage; pogledajmo svaku od njih redom:

- **Prihvatljivost**: Svi dokazi relevantni za slučaj smatraju se prihvatljivim samo ako su relevantni za sporne činjenice slučaja i ne krše zakone ili zakonske statute.
- **Redosled nepostojanosti**: Recimo da ste vatrogasac i da ste stigli do kuće u plamenu; možete da spasite samo jedan po jedan predmet, a u kući se nalaze dva predmeta. Prvi je sneško belić, a drugi je goveđe rebro. Sada ste u dilemi: koji da odaberete? Lako! Prvo spasite sneška jer se topi, a goveđe rebro pustite da se još malo peče da bi ostali vatrogasci imali lepu večeru! Dakle, kada želimo da utvrdimo redosled nepostojanosti, prvo želimo da obezbedimo najkvarljivije dokaze. Ne pokušavamo da zaustavimo napad sve dok ne obezbedimo nestabilne dokaze da bi mogli da identifikujemo izvor. To je poznato kao redosled nepostojanosti. Pogledajmo nekoliko primera.

  *Primer 1* – **Napad zasnovan na vebu**: Napadač napada veb sajt kompanije, a tim za bezbednost pokušava da uhvati mrežni saobraćaj da bi pronašao izvor napada. To je najnestabilniji dokaz.

  *Primer 2* – **Napad unutar računara**: Kada je neko napao vaš računar, morate da hvatate dokaze u skladu sa redosledom nestabilnosti:

  a. **CPU keš**: Brzi blok nestalne memorije koju koristi CPU
  b. **RAM memorija**: Nestalna memorija koja se koristi za pokretanje aplikacija
  c. **Swap/Page File/Virtuelna memorija**: Koristi se za pokretanje aplikacija kada je RAM potrošen.
  d. **Hard disk**: Podaci u mirovanju, koristi se za čuvanje podataka

  *Primer 3* – **Prenosivi disk za skladištenje priključen na računar/server**: Neko je ostavio USB fleš disk priključen na vaš fajl server. Kada je u upotrebi, programi kao što je Word pokreću se u RAM-u, tako da bismo prvo uhvatili nestabilnu memoriju.

*Primer 4* – **Alatke komandne linije**: Morate da znate koji alat komandne linije pruža informacije koje bi mogle da nestanu ako ponovo pokrenete računar, a to je alat `netstat`. Pomoću komande `netstat-an`, prikazani su portovi za osluškivanje i uspostavljeni portovi. Ako ponovo pokrenete računar, sve uspostavljene veze će biti izgubljene.

Redosled nepostojanosti je da se prvo prikupljaju najkvarljiviji dokazi. U napadu zasnovanom na vebu, trebalo bi da prikupljamo mrežni saobraćaj pomoću prisluškivanja paketa.

## Petominutna praksa

Otvorite komandnu liniju na računaru i otkucajte `netstat -an`. Sada bi trebalo da vidite portove za osluškivanje i uspostavljene portove; prebrojte ih i zapišite brojeve. Pokrenite `shutdown /r /t 0` komandu da biste odmah ponovo pokrenuli mašinu. Ponovo se prijavite, otvorite komandnu liniju i pokrenite komandu `netstat -an`; koja je razlika? Videćete da ste izgubili informacije koje su mogle da posluže kao dokaz.

## Prikupljanje dokaza

U ovom odeljku ćemo opisati različite vrste prikupljanja dokaza:

- **E-Discovery**: Tokom e-discovery-ja, dobavljači cloud usluga (CSP) mogu da dobiju sudski poziv da bismo mogli da prikupljamo, pregledamo i tumačimo elektronske dokumente koji se nalaze na hard diskovima, USB drajvovima i drugim oblicima skladištenja.
- **Lanac nadzora**: Lanac nadzora je jedan od najvažnijih aspekata digitalne forenzike, koji osigurava da su dokazi prikupljeni i da nema prekida u lancu. Ovaj lanac počinje kada su dokazi prikupljeni, spakovani, vezani i označeni, što osigurava da dokazi nisu promenjeni. U njemu su navedeni dokazi i ko je njima rukovao. Na primer, narednik Smit je predao 15 kg ilegalne supstance naredniku Džonsu nakon racije sa drogom. Međutim, kada je dokazni materijal predat u prostoriju za dokaze, nedostajao je 1 kg. U tom slučaju, morali bismo da istražimo lanac nadzora. U ovom scenariju, narednik Džons bi bio odgovoran za gubitak. Primeri lanca nadzora su sledeći:

  *Primer 1* – **Nedostaje unos u dokumentu o lancu nadzora**: U ponedeljak je sistemski administrator prikupio 15 laptopova. Sledećeg dana administrator sistema ih je prosledio IT menadžeru. U sredu, IT direktor predstavlja 15 laptopova kao dokaz sudu. Sudija gleda dokument o lancu

nadzora i primećuje da nije bilo formalne primopredaje između IT menadžera i IT direktora. Pošto primopredaja nedostaje, sudija želi da istraži lanac nadzora.

*Primer 2* – **Detektiv ne poseduje dokaz**: FBI hapsi poznatog kriminalca i prikuplja 43 hard diska koje su upakovali i označili, pre nego što ih stave u dve torbe. Oni hapse zločinca i avionom ga odvode iz Arizone u Njujork. Jedan detektiv je vezan lisicama za kriminalca dok drugi nosi dve torbe.

Kada su stigli na čekiranje, službenik avio-kompanije im kaže da su ručne torbe teže od dozvoljene težine i da moraju da idu u skladište. Detektiv pristaje, ali zaključava kofere da spreči krađu. Pošto dokazi nisu fizički u njihovom posedu sve vreme, lanac nadzora je prekinut jer postoji šansa da bi neko ko radi za avio-kompaniju mogao da menja dokaze. Stoga, oni ne mogu da dokažu sudu da je integritet dokaza u svakom trenutku bio netaknut.

- **Poreklo**: Kada je lanac nadzora pravilno sproveden i originalni podaci koji su predočeni sudu nisu menjani, to se naziva poreklo podataka.
- **Zakonsko zadržavanje**: Zakonsko zadržavanje je proces zaštite svih dokumenata, koji mogu da se koriste kao dokaz, od promene ili uništenja. Ponekad je to poznato i kao parnično zadržavanje.

  *Primer*: Dr Death je pacijentima u velikoj bolnici koji su umirali prepisivao nove lekove. Revizor je poslat da istraži mogućnost prekršaja, a zatim, nakon revizije, o tome je obavešten FBI. Doktor je slao e-poštu farmaceutskoj kompaniji koja je isporučivala lekove za ispitivanje. FBI ne želi da doktor bude upozoren, pa su obavestili bolnički IT tim da njegovo poštansko sanduče postave na zakonsko zadržavanje. Kada je poštansko sanduče na zakonskom zadržavanju, ograničenje poštanskog sandučeta se ukida; doktor i dalje može da šalje i prima mejlove, ali ne može ništa da izbriše. Na taj način se ne upozorava na činjenicu da je pod istragom.
- **Prikupljanje podataka**: To je proces prikupljanja svih dokaza sa uređaja, kao što su USB fleš drajvovi, kamere i računari; i podataka u papirnom obliku, kao što su pisma i bankovni izvodi. Prvi korak u prikupljanju podataka je prikupljanje nestalnih dokaza da bi bili sigurni. Podaci moraju da budu spakovani i označeni i uključeni u evidenciju dokaza.
- **Artefakti**: To mogu da budu fajlovi evidencije, grane registra, DNK, otisci prstiju ili vlakna odeće koja su obično nevidljiva golim okom.
- **Vremensko odstupanje**: Kada prikupljamo dokaze sa računara, trebalo bi da zabeležimo vremensko odstupanje. To je regionalno vreme tako da u multinacionalnoj istrazi možemo da ih postavimo u vremenski niz - to je poznato kao normalizacija vremena.

- **Normalizacija vremena**: Ovde se prikupljaju dokazi u više vremenskih zona, a zatim se koristi zajednička vremenska zona, kao što je GMT, da se poređaju u smislen niz.

  *Primer*: Policija u tri različite zemlje pokušava da identifikuje odakle su podaci krenuli u lancu, a zatim ko je upravljao podacima duž linije. Imaju sledeće informacije o tome kada je prvi put kreiran:

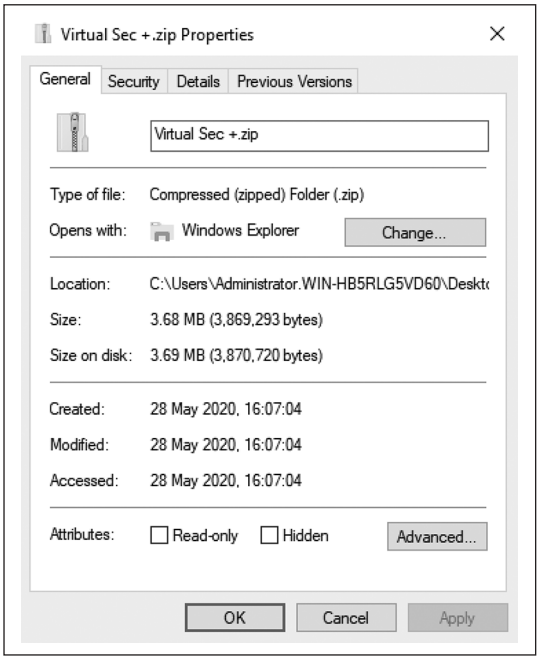
  a. **Njujork**: Kreiran u 3 am

  b. **London**: Kreiran u 4 am

  c. **Berlin**: Kreiran u 4.30 am

  Beleženjem vremenskog razmaka izgleda kao da je počelo u Njujorku, ali ako primenimo normalizaciju vremena, kada je u Londonu 4 ujutro, vreme u Njujorku je 23 sata dan ranije, tako da ne može biti Njujork. Kada je u Berlinu 4.30, u Londonu je samo 3.30; dakle, fajl je nastao je u Berlinu. To je izgledalo najmanje verovatno pre nego što je na vremensko odstupanje prikupljanja podataka primenjena normalizacija vremena.

- **Vremenske oznake**: Svaki fajl ima vremenske oznake koje pokazuju kada su fajlovi kreirani, poslednji put modifikovani i kada im se poslednji put pristupilo:




**Slika 1.7** – Vremenske oznake

- **Forenzičke kopije**: Ako bismo analizirali podatke uskladištene na prenosivom uređaju koji smo nabavili, prvo bismo uzeli forenzičku kopiju i sačuvali originalne podatke netaknute. Zatim bismo koristili kopiju za analizu podataka da bismo originalne podatke sačuvali nepromenjenim, jer ih je potrebno koristiti u originalnom stanju i predočiti sudu kao dokaz. Podaci će biti heširani na početku i na kraju da bi se potvrdilo da dokazi nisu promenjeni.
- **Snimanje sistemskih imidža**: Kada policija uzima dokaze sa laptopova i stonih računara, kreira se kompletan imidž sistema. Originalni imidž se čuva netaknut, a imidž sistema se analizira da bi se pronašli dokazi o bilo kakvoj kriminalnoj aktivnosti. Biće instaliran na drugom računaru i heširan na početku i na kraju da bi se potvrdilo da dokazi nisu promenjeni.
- **Upravljački softver**: Napadač može da izvrši obrnuti inženjering na upravljačkom softveru, koji ponekad nazivamo i ugrađen softver, stoga moramo da uporedimo izvorni kod koji je programer napisao sa trenutnim izvornim kodom u upotrebi. Možemo da zaposlimo stručnjaka za kodiranje da uporedi obe serije izvornog koda tehnikom regresionog testiranja. Tipovi napada koji utiču na ugrađen softver mogu da budu rootkit i backdoor.
- **Snimci**: Ako je dokaz sa virtuelne mašine, snimak virtuelne mašine može da se eksportuje radi istrage.
- **Snimci ekrana**: Takođe možete da kreirate snimke ekrana aplikacija ili virusa na desktopu i da ih zadržite kao dokaz. Bolji način da se to uradi je da upotrebite moderan pametan telefon koji bi geografski označio dokaze.

Trebalo bi da snimite imidž sistema sa laptopa i upotrebite forenzičku kopiju sa prenosivog diska

- **Korišćenje he**ševa: Kada se analizira forenzička kopija ili imidž sistema, podaci i aplikacije se heširaju na početku istrage. Može se koristiti kao kontrolni zbir da bi se osigurao integritet. Na kraju se ponovo hešira i trebalo bi da se podudara sa originalnom heš vrednošću da bi se dokazao integritet podataka.
- **Mrežni saobraćaj i evidencije**: Kada istražujemo napad zasnovan na vebu ili udaljeni napad, prvo bi trebalo da uhvatimo promenljiv mrežni saobraćaj pre nego što zaustavimo napad. To će nam pomoći da identifikujemo izvor napada. Pored toga, trebalo bi da pogledamo različite fajlove evidencije iz firewall-a, NIPS-a, NIDS-a i bilo kog uključenog servera. Ako koristimo **Security Information Event Management** (**SIEM**) sistem, to može da

pomogne u sastavljanju tih unosa i da pruži dobru sliku o svakom napadu. Međutim, ako se radi o virusu koji se brzo širi, staviljamo ga u karantin.

*Primer*: Vaša kompanija koristi zaključavanje naloga nakon tri pokušaja. Ako napadač pokuša da se prijavi jednom na tri odvojena računara, svaki računar to ne bi identifikovao kao napad, jer je to jedan pokušaj na svakom računaru, ali SIEM sistem će ove pokušaje smatrati kao tri neuspela pokušaja prijave i upozoriti administratore u realnom vremenu.

Trebalo bi odmah da uklonite računar sa virusom koji se dinamički širi umesto da prikupljate mrežni saobraćaj.

- **Snimanje video zapisa**: CCTV može da bude dobar izvor dokaza koji pomaže u identifikaciji napadača i vremena kada je napad pokrenut. To može da bude od vitalnog značaja za hapšenje osumnjičenih.
- **Intervjui**: Policija takođe može da uzme izjave svedoka da bi pokušala da dobije sliku o tome ko je bio umešan i možda onda koristi foto-fitove da bi osumnjičeni mogli da budu uhapšeni.
- **Čuvanje**: Podaci moraju da budu sačuvani u originalnom stanju da bi mogli da se iznesu kao dokaz na sudu. Zbog toga uzimamo kopije i analiziramo kopije tako da se originalni podaci ne menjaju, odnosno da ostanu netaknuti. Stavljanje kopije najbitnijeg dokaza u WORM disk će sprečiti bilo kakvo neovlašćeno menjanje dokaza, jer podaci sa WORM disk jedinice ne mogu da se brišu. Takođe, diskove za skladištenje možete da zaštitite od pisanja.
- **Oporavak**: Kada je incident iskorenjen, možda ćemo morati da povratimo podatke iz rezervne kopije; brži metod bi bio „vrući“ sajt koji je već pokrenut sa podacima starim manje od 1 sata. Možda ćemo morati da kupimo i dodatni hardver ako je originalni hardver oštećen tokom incidenta.
- **Strateško obaveštajno/kontraobaveštajno prikupljanje**: Ovde različite vlade razmenjuju podatke o sajber kriminalcima da bi mogli da rade zajedno na smanjenju pretnji. Takođe je moguće da kompanije koje su pretrpele napad zabeleže što više informacija i da imaju treću stranu koja je specijalizovana za odgovaranje na incidente da im pomogne da pronađu način da spreče ponovnu pojavu.
- **Aktivno evidentiranje**: Da bismo pratili incidente, potrebno je da aktivno nadgledamo i aktivno evidentiramo promene obrazaca u fajlovima evidencije ili obrazaca saobraćaja u našoj mreži. Instaliranje SIEM sistema koji obezbeđuje nadgledanje u realnom vremenu može da pomogne u prikupljanju svih unosa u fajlovima evidencije, obezbeđujući da se ne

koriste dupli podaci da bi se mogla napraviti prava slika. Upozorenja zasnovana na određenim okidačima mogu da se podese na SIEM sistemu tako da budemo obavešteni čim se događaj desi.

## Cloud forenzika

U poslednjih nekoliko godina, rast cloud računarstva i resursa se povećava iz godine u godinu. Cloud forenzika ima drugačije potrebe od tradicionalne forenzike. Jedan od primarnih aspekata koje cloud provajder mora da obezbedi jeste bezbednost podataka uskladištenih u cloud-u.

Godine 2012. kreiran je Cloud Forensic Process 26 za fokusiranje na nadležnost i prihvatljivost dokaza. Faze su sledeće:

- **Faza A –** Provera svrhe cloud forenzike.
- **Faza B –** Provera vrste cloud servisa.
- **Faza C –** Provera vrste tehnologije koja stoji iza cloud-a.
- **Faza D –** Provera uloge korisnika i pregovaranje sa **dobavljačem cloud usluga** (**CSP**) za prikupljanje potrebnih dokaza.

Cloud servisi, zbog prirode svog poslovanja, kreiraju virtuelne mašine, a zatim ih redovno uništavaju. To onemogućava prikupljanje forenzičkih dokaza. Forenzički tim treba da dokaže cloud provajderu svoje razloge za prikupljanje dokaza i mora da se osloni na to da će mu cloud provajder poslati ispravne dokaze koji su mu potrebni.

### Klauzule o pravu na reviziju

Umetanjem klauzula o pravu na reviziju u ugovore o lancu snabdevanja, revizor može da poseti prostorije bez prethodne najave i da pregleda knjige i evidenciju izvođača da bi se uverio da ugovarač ispunjava svoje obaveze iz ugovora. To bi im pomoglo da identifikuju sledeće:

- Neispravan ili loš kvalitet robe
- Kratke pošiljke
- Roba nije isporučena
- Povratni udari
- Pokloni i napojnice zaposlenima u kompaniji
- Provizije brokerima i drugima
- Navodno izvršene usluge koje nisu bile potrebne, kao što je popravka opreme

### Regulativa i nadležnost

Cloud podaci bi trebalo da se čuvaju i da imaju suverenitet podataka u regionima. SAD su uvele CLOUD Act 2018. godine zbog problema sa kojima se FBI suočio kada je primorao Microsoft da preda podatke uskladištene u Irskoj. Godine 2019. Velika Britanija je dobila kraljevsku saglasnost za Zakon o proizvodnji u inostranstvu (COPOA), koji omogućava Velikoj Britaniji da traži podatke uskladištene u inostranstvu u okviru krivične istrage. Godine 2019. SAD i Velika Britanija potpisale su sporazum o razmeni podataka da bi se agencijama za sprovođenje zakona u svakoj zemlji omogućio brži pristup dokazima koje drže provajderi, kao što su društveni mediji ili veb hosting. Godine 2016. sličan sporazum je postavljen između SAD i EU; međutim, uvođenjem **Opšte uredbe** o zaštiti podataka (**GDPR**), sve veb stranice u SAD koje imaju potrošače iz EU moraju da se pridržavaju GDPR-a.

### Obaveštenja o kršenju podataka/zakona

Ako dođe do povrede podataka, kompanija može da bude kažnjena sa više od 10 miliona funti jer nije prijavila kršenje. EU koristi GDPR, a obaveštenja o kršenju podataka moraju da budu prijavljena u roku od 72 sata. Druge zemlje imaju svoj vremenski okvir za izveštavanje.

## Pitanja za ponavljanje gradiva

Sada je vreme da proverite svoje znanje. Odgovorite na sledeća pitanja i proverite svoje odgovore koji se nalaze u odeljku *„Rešenja“* na kraju knjige:

1. Koje su tri komponente CIA trijade?
2. Zašto neaktivna CCTV kamera može da se postavi na spoljni zid zgrade?
3. Šta znači poverljivost?
4. Kako možete da kontrolišete pristup osoblja data centru?
5. Koja je svrha vazdušnog zazora?
6. Navedite tri glavne kontrolne kategorije.
7. Navedite tri fizičke kontrole.
8. Nakon incidenta, koja vrsta kontrole se koristi prilikom istraživanja kako se incident dogodio?
9. Kako znate da li je integritet vaših podataka netaknut?
10. Šta je ispravljačka kontrola?

**11.** Koja je to vrsta kontrole kada promenite pravila firewall-a?

**12.** Šta se koristi za prijavljivanje na sistem koji radi zajedno sa PIN-om?

**13.** Kako se zove osoba koja vodi računa o poverljivim podacima? Ko ljudima daje pristup poverljivim podacima?

**14.** Kada koristite DAC model za pristup, ko određuje ko dobija pristup podacima?

**15.** Šta je najniža privilegija?

**16.** Kakav pristup daje dozvola 764 za Linux fajl?

**17.** Prodajnom timu je dozvoljeno da se prijavi u sistem kompanije između 9 i 22 sata. Koji tip kontrole pristupa se koristi?

**18.** Samo dve osobe iz finansijskog tima mogu da autorizuju isplatu čekova. Koju vrstu kontrole pristupa koriste?

**19.** Koja je svrha detaljnog modela odbrane?

**20.** Kada neko napusti kompaniju, šta bi prvo trebalo da uradite sa njegovim korisničkim nalogom?

**21.** Čega treba da se pridržavaju američke kompanije koje hostuju veb-sajtove u SAD ako se klijenti nalaze u Poljskoj?

**22.** Kako kompanija može da otkrije da njeni dobavljači koriste inferiorne proizvode?

**23.** Koji je jedan od najvažnijih faktora da neko bude uhapšen i da se pojavi pred sudijom na sudu?

**24.** Možete li da objasnite koja je svrha CLOUD Act-a i COPOA-a?

**25.** Šta je faza C Cloud Forensic Process-a 26?