XIII – Organizacione, pravne i fizičke mere zaštite

S A D R Ž A J

1. Osnovni pojmovi
2. Procena rizika
3. Organizacione mere zaštite
4. Fizičke metode zaštite
5. Pravne metode zaštite

13.1 – Osnovni pojmovi

- Podaci i informacioni sistemi su izloženi velikom broju pretnji koje mogu dovesti do značajnih gubitaka informacije ili oštećenja opreme.
- Pretnja je definisana kao fenomen koji može da prouzrokuje štetu.
- Pretnje mogu nastati kako iz spoljnih tako i iz unutrašnjih izvora: smišljenim postupcima čija su meta informaciona dobra, ljudskom greškom koja može dovesti do slučajnog oštećenja informacionog dobra i usled havarija ili prirodnih nepogoda.
- Pretnje se neprekidno menjaju, kako se poslovanje organizacije menja.
- Ispitivanjem je otkriveno da zaposleni ili saradnici u okviru organizacije najviše narušavaju sigurnost.
- Pretnje zloupotrebljavaju ranjivosti informacionih dobara.
- Ranjivost je slabost fizičkog okruženja, organizacije i upravljanja, procedura, osoblja,operacija,hardvera,komunikacione opreme, softvera
- Većina značajnih ranjivosti nastaje kada su kontrole sigurnosti, ili nepravilno konfigurisane ili nisu pravovremeno ažurirane
- Neke pretnje i ranjivosti mogu da utiču na jedno ili više informacionih dobara pa samim tim i posledice mogu biti različite.

13.1 – Osnovni pojmovi

- Kada se govori o sigurnosti računarskih mreža najčešće se govori o tehničkim i programskim metodama, koje se prvenstveno odnose na primenu raznovrsnih softverskih i hardverskih rešenja.
- Postoji i druga grupa mera, koje su podjednako važne za sigurnost
- Taj skup mera obuhvata organizacione, fizičke i pravne metode zaštite.
- Ove mere se primenjuju zajedno sa tehničkim, programerskim i kriptografskim metodama i tako se ostvaruje kompletan efekat zaštite
- Kontrola sigurnosti informacija je neuporedivo jeftinija i efikasnija ako se objedini u jedan sistem, koji ispunjava neophodne specifikacije
- Od suštinske važnosti je da organizacije definišu sigurnosne zahteve:

1. **Utvrđivanje rizika po organizaciju** - određuju se pretnje po sredstva te organizacije, koliko je ona ranjiva na napade, koja je verovatnoća da se nešto desi, kao i kolika bi u tom slučaju mogla da bude šteta.
2. **Pravni, statutarni, regulativni i ugovorni preduslovi**
3. **Konkretan komplet principa, ciljeva i preduslova za obradom informacija** koje organizacije razvijaju

13.1 – Osnovni pojmovi

- Sigurnosni preduslovi se otkrivaju metodološkim utvrđivanjem bezbednosnih rizika.
- Treba predvideti i troškove koje onda treba uporediti sa potencijalnom štetom do koje bi došlo ako nikakve zaštite ne bi bilo.
- Tehnike utvrđivanja rizika mogu da se primene na celu organizaciju ili samo za neke njene delove, kao i za pojedinačne informacione sisteme,
- Da bi se obezbedila čvrsta osnova za određivanje zahtevanog nivoa zaštite, informacije se obeležavaju u skladu sa klasifikacijom po sigurnost na osnovu kriterijuma.
- Cilj klasifikacije je identifikovanje informacionih dobara koje su od vitalnog značaja za funkcionisanje organizacije.
- Jedan od najvažnijih zadataka u procesu sigurnosti informacija je analiza rizika koja obuhvata sledeće aspekte:
  - ✓ potencijalnu štetu do koje će najverovatnije doći ako sigurnosne mere zakažu, pri čemu treba uzeti u obzir potencijalne posledice,
  - ✓ sasvim je realno očekivati da će do takvih padova doći ako sigurnost nije adekvatna, a slabosti i nedostataka ima previše

13.1 – Osnovni pojmovi

- Rezultat ove procene pomoći će da se odrede koraci koje rukovodstvo treba da preduzme i prioriteti u upravljanju sigurnosnim merama, kao i u primeni tih mera koje se i biraju da bi ti rizici bili što manji.
- Sam proces utvrđivanja rizika i odabira kontrolnih mera možda treba da se izvrši više puta da bi se pokrila cela organizacija
- Na raznim nivoima treba vršiti preglede stanja u zavisnosti od rezultata prethodnog utvrđivanja pa rukovodstvo treba da bude spremno na promene i prilagođavanje sigurnosnog sistema.
- Procena rizika se prvi put najčešće vrši na vrlo visokom nivou, jer se jedino tako resursi mogu svrstati po prioritetima
- Čim se identifikuju svi sigurnosni preduslovi, treba pristupiti odabiru i realizaciji kontrole da bi se rizici sveli na što je moguće manju meru.
- Kontrole se biraju na osnovu troškova realizacije kao i sa smanjenjem rizika i potencijalnim gubicima kod narušavanja bezbednosti
- Postoji mnogo kontrolnih mera koje se zasnivaju ili na ključnim zakonskim preduslovima ili se smatraju naboljim rešenjem kada se radi o sigurnosti informacija.

13.1 – Osnovni pojmovi

- Mere koje su sa pravne tačke gledišta od ključne važnosti obuhvataju:
  - zaštitu podataka i privatnosti ličnih informacija,
  - čuvanje organizacionih podataka,
  - zaštitu intelektualne svojine.
- Kontrolne mere koje se smatraju najčešćim i najboljim rešenjima sigurnosti informacija su:
  - dokument koji sadrži politiku sigurnosti informacija,
  - određivanje stepena odgovornosti za sigurnost informacija,
  - edukacija i obuka po pitanju sigurnosti informacija,
  - prijavljivanje sigurnosnih incidenata,
  - upravljanje kontinuitetom poslovanja,
  - zaštita i otkrivanje virusa i drugih štetnih softvera.

13.1 – Osnovni pojmovi

➢Iskustvo je pokazalo da su sledeći faktori često od suštinske važnosti za uspešnu realizaciju sigurnosti informacija u okviru jedne organizacije:

- ✓ sigurnosna politika, ciljevi i aktivnosti koji se odražavaju na poslovnu strategiju,
- ✓ pristup realizaciji sigurnosnih mera koji je u skladu sa organizacionom strukturom,
- ✓ vidljiva podrška i posvećenost rukovodilaca,
- ✓ dobro razumevanje sigurnosnih preduslova, utvrđivanja rizika i upravljanja rizicima,
- ✓ efikasno promovisanje sigurnosnih mera kod rukovodilaca i zaposlenih
- ✓ distribucija priručnika o informacijama koje se tiču politike sigurnosti i standarda koji važe za sve zaposlene,
- ✓ obezbediti odgovarajuću obuku i edukaciju,
- ✓ uspostaviti sveobuhvatan i uravnotežen sistem procene koji se koristi da se utvrde performanse u upravljanju merama sigurnosti i dobiju povratne informacije kao što su predlozi za eventualno poboljšanje.

13.2 – Procena rizika

- U kreiranju politike sigurnosti postoji potreba da se znaju rizici
- Rizik je mera opasnosti odnosno mogućnost da nastane oštećenje ili gubitak neke informacije, hardvera, intelektualne svojine, prestiža ili ugleda i definiše se eksplicitno:

Rizik = Pretnja x Ranjivost x Vrednost imovine

- ***Pretnja*** je protivnik (haker), situacija (zemljotres, požar) ili splet okolnosti (greška operatera) sa mogućnostima da ekspoatiše ranjivost.
- ***Ranjivost*** je slabost u nekoj vrednosti, resursu ili imovini koja može biti iskorišćena.
- ***Vrednost imovine*** je mera vremena i resursa potrebnih da se neka imovina zameni ili vrati u svoje prethodno stanje.

- Osetljivost sistema na neki događaj definiše se kao finansijski gubitak koji pretrpi neka organizacija ako se taj događaj desi.
- Izloženost sistema nekom događaju (rizik) definiše se kao osetljivost na taj događaj, pomnožena verovatnoćom njegovog dešavanja.
- Verovatnoća rizika određuje vremenski interval u kome se očekuje jedno dešavanje tog događaja

13.2 – Procena rizika

- Kada korisnik odlučuje kako će reagovati na rizik, on može da bira:

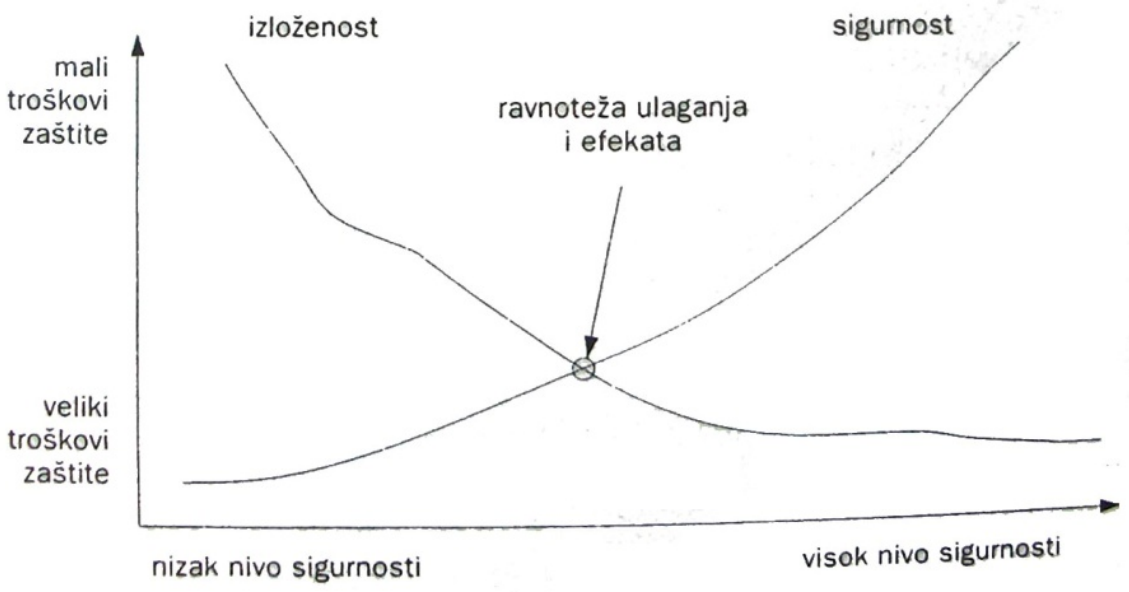
1. Prihvatiti rizik - ako je izloženost mala a troškovi zaštite velike, vaša politika sigurnosti možda može prihvatiti rizik.
2. Dodeliti rizik - kupovanje zaštite od neke druge komercijalne firme.
3. Izbeći rizik - uspostavljanje sigurnosnih mera tako da je verovatnoća pojave incidenta jako mala.

- Procena rizika (*risk assessment*) prvenstveno je okrenuta pretnjama, "ranjivim" mestima i posledicama eventualnog narušavanja rada sistema za obradu podataka, odnosno gubitka podataka.
- Svaki utvrđeni rizik mora biti definisan, opisan i procenjen sa stanovišta mogućnosti da će nastupiti.
- Procena rizika obuhvata sledeće aktivnosti:

1. ***Definisanje mogućih rizika.***
2. ***Utvrđivanje rizika koji zaslužuju posebnu pažnju.***
3. ***Koordinacija sa planovima za hitne slučajeve.***

13.2 – Procena rizika

- Upravljanje rizikom je proces uravnotežavanja troškova za zaštitu od rizika i troškova od izloženosti riziku.
- Kada su trošak za zaštitu od rizika i trošak izloženosti riziku skoro jednaki - u istoj tački, kao što je ilustrovano na slici, mere sigurnosti IT sistema su uravnotežene i promišljene na odgovarajući način.
- U drugim slučajevima, u firmi se može potrošiti znatno više na sigurnost IT sistema nego što iznosi sam korisni efekat koji daje upravljački informacioni sistem, ili što je verovatnije - ulaže se premalo, čime se firma nepromišljeno izlaže riziku.



13.3 – Organizacione mere zaštite

- Organizacione mere zaštite podrazumevaju postojanje strukture koja je odgovorna za celokupni sistem zaštite.
- Struktura mora definisati koordinatore u pogledu zaštite, odgovarajuće delegiranje obaveza sistema upravljanja i procese reakcije na incidente
- Organizovanje informacione sigurnosti zahteva da se jasno odredi sve odgovornosti svih u skladu sa sigurnosnom politikom.
- Rukovodeći ljudi organizacije trebaju da podrže uspešno sprovođenje sigurnosne politike, ali i na propisan način kažnjavaju prekršioce.
- Koraci koji se poduzimaju pri organizaciji informacione sigurnosti su:
  - proces autorizacije
  - ugovor o poverenju
  - saveti stručnjaka za informacionu sigurnost
  - saradnja sa drugim organizacijama
  - provera sigurnosti sistema
  - sigurnost pristupa treće stane
  - identifikacija rizika kod pristupa treće strane
  - zahtevi sigurnosti u ugovorima sa trećom stranom

13.3 – Organizacione mere zaštite

- Prilikom projektovanja i realizovanja informacionih sistema i računarskih mreža, treba voditi računa o skupu mera za povećanje sigurnosti i održavanje rizika na prihvatljivom nivou, uz prihvatljive troškove i uticaj na performanse sistema pa je potrebno definisati:
  - **odgovornost u projektovanju tehnika i postupaka zaštite**
    - celokupnu koordinaciju, odgovornost za tehnički aspekt projekta,
    - odgovornost za proceduralne kontrole,
    - odgovornost za kontrolu programa i programera,
    - odgovornost za fizičku zaštitu,
    - odgovornost za proveru funkcionisanja sistema zaštite.
  - **odgovornost za zaštitu pri svakodnevnom radu**.
  - **odgovornost za proceduralne kontrole**:
    - operativne procedure i kontrole,
    - rad u prostoriji s računarima,
    - procedure i pravila kojima se štite podaci,
    - procedure potrebne prilikom zamene starog sistema novim,
    - procedure koje se primenjuju u slučajevima otkaza računa.sistema

13.3 – Organizacione mere zaštite

- Podrazumevamo projektovane i preduzete mere koje se odnose na povećanje sigurnosti i održanje prihvatljivog nivoa rizika tokom rada uz minimiziranje troškova potrebnih za njihovu implementaciju
- U fazi projektovanja potrebno je obratiti pažnju na:
  - precizno definisanje ciljeva koje želimo postići
  - načine i metode postizanje tih ciljeva
  - načine i metode održavanja postignutog
  - tehničko rešenje sa predviđenim proširenjima
  - kadrovsku strukturu sa preciznim zaduženjima po radnim mestima
  - vremensko trajanje projektovanog stanja.
- U delu koji se bavi održanjem prihvatljivog sigurnosnog rizika treba da se definišu:
  - tehnički sigurnosni sistemi zaštite sa tempom unapređenja
  - kadrovska politika pristupa informacijama od značaja
- Kada se radi o minimizaciji troškova i maksimizaciji raspoloživosti sistema onda treba naglasiti da se uvek teži minimalnom ulaganju

13.3 – Organizacione mere zaštite

- Prilikom realizacije zaštite, potrebno je obaviti čitav niz mera i to:
  - opšta kontrola i raspitivanje,
  - korišćenje upitnika i anketa,
  - povremene najavljene i nenajavljene provere,
  - namerna primena pogrešnih transakcija i generalno "provociranje" reakcije na grešku,
  - pokušaji narušavanja integriteta, tajnosti i raspoloživosti elemenata sistema i sistema u celini,
  - raznovrsna ispitivanja, pilot sistemi, specijalni programi za nadzor, analize, simulacije,
  - procedure za traženje grešaka (*troubleshooting*).
- Navedene mere, kao i brojne druge, poboljšavaju celokupnu sigurnost računarskih sistema, mreža i informacionih sistema u celini.
- Potrebno je osmisliti i povremeno sprovoditi kompletno ili delimično ispitivanje radi provere zaštite.

13.3 – Kadrovski aspekti

- Efikasno upravljanje sistemom zaštite zahteva jasno definisanje uloga i obaveza za sve osobe koje su uključene u taj proces:

1. **Vlasnik** (*owner*) podataka je prvenstveno odgovoran za njihovu zaštitu i upotrebu. Kod većine slučajeva to je neko od viših organa upravljanja ili neka druga osoba zadužena za donošenje odluka u organizaciji
2. **Čuvar** (*custodian)* podataka je zadužen za njihovo održavanje i zaštitu. Kada je reč o računarima, tu ulogu obično dobija IT odeljenje.
3. **Korisnik** (*user*) je osoba koja upotrebljava podatke. On obično obavlja funkcije unosa podataka, njihovog izvoza i editovanja, kao i druge funkcije koje su dodeljene toj ulozi.
4. **Revizori** (*auditor*) su zaduženi za kontrolu sprovođenja propisanih procedura, pravila i mehanizama u okviru organizacije.

- Takav posao obično zahteva pregled dokumentacije i log datoteka i obavljanje razgovora sa zaposlenima, uz brojne druge zadatke radi provere poštovanja propisa u okviru organizacije.
- Revizor nije policijski inspektor, već samo konsultant.
- On pomaže organizaciji u otkrivanju propusta u sistemu zaštite.

13.3 – Kadrovski aspekti

- Potrebno je voditi računa i o kadrovskim pitanjima odnosno o pravima prisupa osetljivim informacijama.
- Iz tog razloga treba se voditi računa o stručnosti, poverenju i lojalnosti postavljenih, pre svega, rukovodećih ljudi a naravno i svih ostalih.
- Kao jedan vid hijarhije odgovornosti definišu se sledeći poslovi:

1. ***rukovodilac*** računskog centra - zadužen za raspodelu poslova i odgovornosti i odgovoran za striktnu i neprikidnu primenu mera zaštite
2. ***administrator*** - manipulacija korisničkim nalozima, dodela i zabrana prava pristupa određenim resursima sistema, praćenje statistike
3. ***lokalni administrator*** - zadužen za deo administratorskih poslova
4. ***supervizor sigurnosti*** - zadužen za periodičnu proveru sigurnosnih mera, predloge za njihovo unapređenje i kontrolu rada samih administratora. Poželjno je da to bude izuzetno stručna osoba koja uz to poseduje i poverenje vlasnika a najbolje je da to bude osoba koja nije zaposlena u sistemu koji kontroliše.
5. ***vlasnici datoteka*** – opciona jer može (ali i ne mora) postojati vlasnik datoteke odnosno baze podataka.

13.4 - Fizičke metode zaštite

- Domen fizičke sigurnosti sistema bavi se pretnjama, ranjivostima i merama koje se mogu primeniti kako bi se fizički zaštitili resursi i poverljive informacije neke kompanije, orgnizacije ili institucije.
- U resurse koji se fizički štite spadaju osoblje, prostorije u kojima osoblje radi, računarska i komunikaciona oprema, medijumi s kojima se radi i pomoćna infrastruktura.
- Fizička sigurnost se najčešće odnosi na mere koje se preduzimaju kako bi se proizvodni i poslovni sistemi zaštitili od pretnji
- Fizičkim merama zaštite sprečava se neovlašćeni pristup mrežnim sistemima,prvenstveno zabranom fizičkog kontakta neovlašćene osobe

Rizik predstavljaju:

- prekidi u obezbedivanju računarskih usluga,
- fizičko oštećenje sistema ili pomoćne infrastrukture,
- neovlašćeno razotkrivanje informacija (poverljivost),
- gubitak kontrole nad sistemom (integritet).
- krađa podataka i/ili opreme (poverljivost, integritet i raspoloživost).

13.4 - Fizičke metode zaštite

Primeri pretnji po fizičku sigurnost:

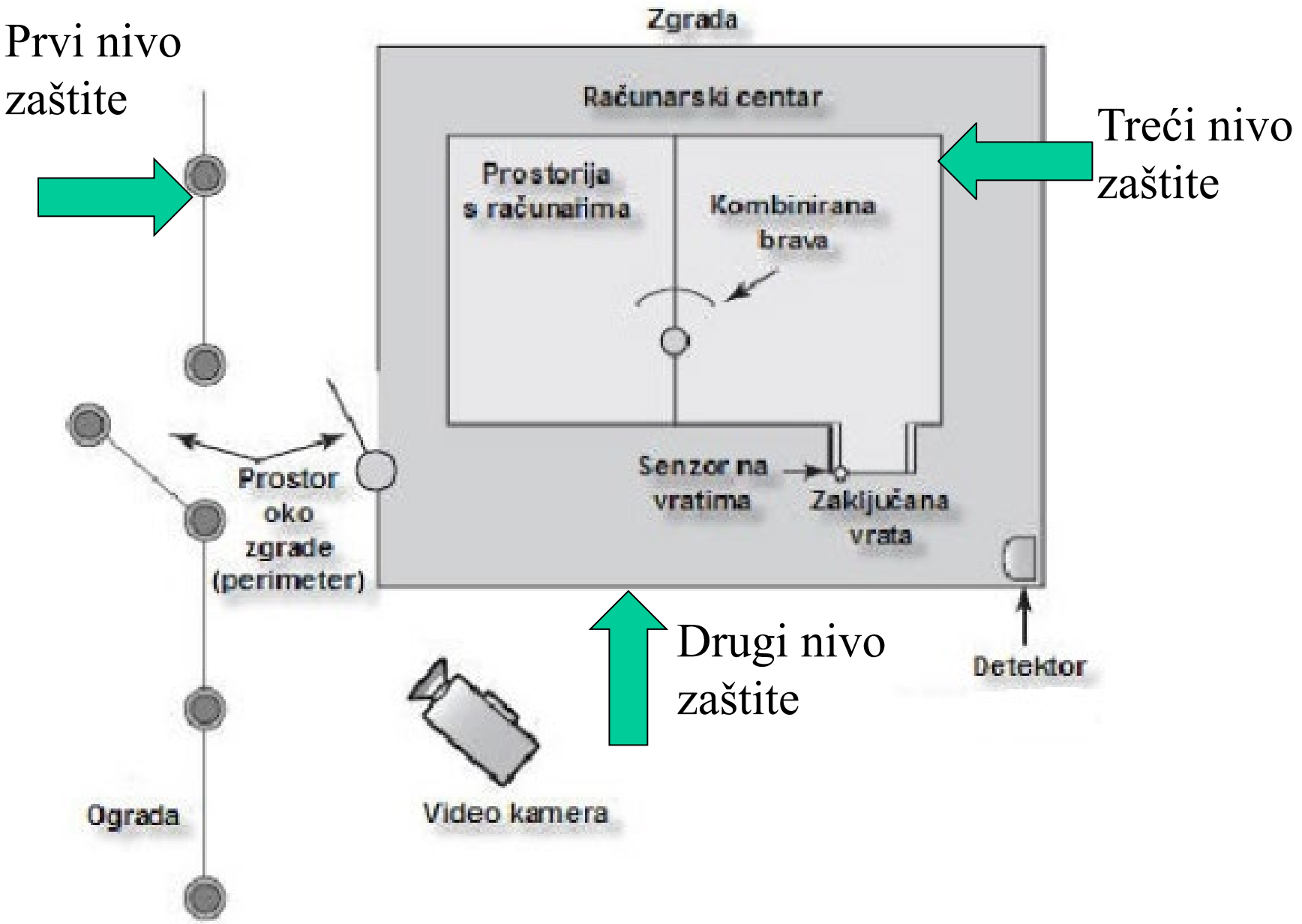
- hitni slučajevi (požari i zagađenje dimom, oštećenje građevine, eksplozije, prekid snabdevanja električnom energijom,
- prirodne katastrofe (zemljotresi, klizišta, poplave).
- ljudska intervencija (sabotaže, vandalizam, ratovi, državni udari).

- Karakteristike fizičke sigurnosti se ogleda u pretnjama, ranjivostima i merama koje se mogu primeniti kako bi se fizički zaštitili resursi i poverljive informacije neke kompanije, organizacije ili institucije.
- U resurse koji se fizički štite spadaju osoblje, prostorije u kojima osoblje radi, računarska i komunikaciona oprema, medijumi s kojima se radi i pomoćna infrastruktura.
- Fizička sigurnost se najčešće odnosi na mere koje se preduzimaju kako bi se proizvodni i poslovni sistemi zaštitili od pretnji kao što su provale i krađa resursa i poverljivih informacija, pa se najednostavnije može definisati kao proces kontrole osoblja, opreme i podataka
- Jedan segment fizičke zaštite je fizička kontrola pristupa prostorijama u kojima se nalaze računari, računarska i komunikaciona oprema.

13.4 - Fizičke barijere

- Predstavljaju osnovu celokupnog sistema kontrole pristupa.
- Sprečavanje pristupa računarima je primarni cilj fizičke kontrole
- Da bi takva kontrola bila što efikasnija, postavlja se više fizičkih prepreka koje treba proći da bi bio ostvaren pristup računar. sistemima
- Takav pristup se često označava kao sistem sa višestrukom fizičkom kontrolom (*multiple barrier svstem*).
- U najboljem slučaju, računar.sistem mora imati bar tri fizičke prepreke
- Prva prepreka je kompletan prostor oko zgrade (*perimeter*), koji se obično štiti alarmnim sistemima, ogradom, video nadzorom i slično
- Druga prepreka je ulaz u rač.centar, koji se nalazi iza zaključanih vrata
- Treća prepreka je ulaz u prostoriju u kojoj se nalaze računari.
- Svi ovi ulazi se mogu zasebno osigurati, nadgledati i zaštititi posebnim alarmnim sistemima.
- Tri navedene barijere neće uvek sprečiti "uljeze", ali će ih sigurno usporiti u dovoljnoj meri ili odvratiti.
- Računarski sistemi sa visokim stepenom zaštite koriste i neki vid srednjeg zaštitnog mehanizma-kontrolne prostorije ili klopke-*mantraps*

13.4 – Tri nivoa fiziče zaštite



13.5 – Pravne metode zaštite

- Pravni aspekt zaštite se odnosi na zakonsku regulativu definisanu kroz interne akte organizacije koja se štiti, kao i kroz zakonska akta države koja su ne retko u disproporciji sa međunarodnim pravnim obavezama
- Primena informacionih tehnologija podstakla je aktivnosti na uvođenju novih pravnih regulativa koja se odnose na područja:

1. zaštitu od *cyber*-kriminala (doneta 2001. godine), obuhvata:
   - krivična dela protiv tajnosti, nepovredivosti i dostupnosti podataka (neovlašćeni pristup, neovlašćeno presretanje podataka, menjanje sadržaja, brisanje ili oštećenje podataka, ometanje normalnog rada računara, proizvodnja, distribucija i upotreba uređaja koji mogu omogućiti neku od prethodnih nedozvoljenih radnji)
   - krivična dela počinjena upotrebom računara (falsifikovanje, prevare)
   - krivična dela širenja neprimerenog materijala (npr. dečja pornografija)
   - kršenje autorskih prava (nad softverom i hardverom)
2. zaštitu privatnosti odnosno baza podataka s podacima građana,
3. računarskog kriminala odnosno raznih zloupotreba računara
4. zaštitu intelektualnog vlasništva (autorska prava, patenti)

13.5 – Pravna zaštita

- Postoje tri vrste svojine:
  1. nepokretna svojina (zemljište, zgrade,...)
  2. lična svojina (lične stvari, pokretna svojina, mali poslovi,...)
  3. intelektualna svojina (vrednost ljudskog znanja i ideja).
- U oblasti bezbednosti računara i mreža, od značaja su različiti oblici intelektualne svojine:

- **softver** (komercijalni i sopstveno razvijeni softveri, kao i softverski prozvodi pojedinaca) se može zaštiti autorskim pravima i patentima
- **baze podataka** (mogu sadržati podatke organizovane na način da imaju komercijalnu vrednost) se mogu štititi autorskim pravima
- **digitalni sadržaj** (audio datoteke, video datoteke, multimedia, sadržaj Web sajtova, i drugi originalni rad u elektronskom obliku)
- **algoritmi** (na primer RSA kriptosistemi) se mogu štititi patentima.

- Postoje tri osnovna tipa intelektualne svojine sa pravnom zaštitom:
  1. robne oznake (neautorizovano korišćenje ili imitacije)
  2. autorska prava (neautorizovano korišćenje)
  3. patenti (neautorizovan izrada, korišćenje i prodaja).

13.5 – Robna oznaka

- Robna oznaka (*trademark*) je reč, ime, simbol ili uređaj koji se koristi u trgovini proizvoda a koji asocira na izvor i jedinstveno ga razlikuje od drugih proizvoda.
- Prava na robnu oznaku se mogu koristiti za sprečavanje korišćenja slične oznake koja dovodi u zabunu kupca, ali ne sprečava ostale da proizvode i prodaju istu robu sa različitom robnom oznakom.

13.5 – Autorsko pravo

- Najkorišćeniji način zaštite intelektualnog vlasništva.
- Autorsko pravo načelno štiti originalnu implementaciju i način prikaza neke ideje, a ne samu ideju.
- Autorsko pravo štiti autora od nelegalnog korišćenja njegovog dela.
- U softverskoj industriji to znači da je moguće autorskim pravom zaštititi izvorni i izvršni kod programa, strukturu i organizaciju koda programa, delove ili ceo korisnički sistem kao i sve priručnike, uputstva i ostalu dokumentaciju u digitalnom ili pisanom obliku.
- Autorsko pravo ne štiti razne programske algoritme ili metode i matematičke postupke koji su korišćeni u realizaciji softvera.
- Autorsko pravo štiti od neovlašćenog kopiranja ili oponašanja koda, ali ne štiti od konkurencije koja samostalno i nezavisno (bez uvida u izvorni kod konkurencije) razvija sličan softver.
- Naprotiv, drugi autor može čak dobiti autorsko pravo za svoj program bez obzira na sličnost s postojećim softverom.
- Autorsko pravo se često koristi jer je primenjivo na skoro svaki oblik softvera, a moguće ga je lako, brzo i jeftino dobiti.

13.5 – Patent

- Predstavlja zaštitu izuma koju izdaje vlada neke države
- Na taj način sprečavaju se druge osobe ili organizacije da proizvode i prodaju isti ili sličan proizvod.
- Patentna zaštita se može primeniti na svaki koristan princip, mehanizam i proizvodni proces koji je nov, nije očigledan i nije deo nijednog prethodno objavljenog patenta.
- Za razliku od autorskog prava, patent zabranjuje objavu bilo kakvog sličnog rada pa makar bio i nezavisno napravljen.
- Za razliku od autorskog prava koje štiti prezentaciju neke ideje i oblik izražavanja, patent štiti samu ideju.
- U softverskoj primeni, patent štiti ideje, algoritme i matematičke postupke korišćene u programu, a ne sam programski kod.
- Patent je dokaz vlasništva pronalazača:

❑ patent korišćenja (dodeljuje se svakom pronalazaču novog i koristnog procesa, mašine, industrijskog proizvoda ili poboljšanja postojećeg)

❑ patent projektovanja (dodeljuje se svakom pronalazaču novog i originalnog projekta industrijskog proizvoda).

13.5 – Licenca

- Predstavlja posebnu dozvolu u kojoj je tačno definisano na koji se način može koristiti taj softver.
- U licenci se definiše na koliko računara se softver sme instalirati, u koje svrhe se sme koristiti (komercijalne, privatne, obrazovne itd.) te koliko dugo je licenca važeća.
- Licenca se mora obnoviti nakon isteka (tj. ponovno kupiti od autora programa) ili klijent mora prestati da koristi softver.
- Korisnik uopšte ne kupuje licenciran softver već samo licencu za njegovo korišćenje, što znači da autor ostaje vlasnik softvera.
- Većina današnjeg softvera se prodaje u vidu licenciranog softvera
- Postoji više vrsta licenciranja softvera

13.5 Vrste licenci

- Pristup serveru se omogućava licencama, takozvanim CAL-ovima (*Client Access License*), koji u suštini predstavljaju dokument kojim se dokazuje legalno pravo pristupa serveru.

•**Per-User:** odnosi se na tačno određenog korisnika. Korisnik može da pristupi serveru sa bilo kog uređaja(desktop klijent,PDA,mobilni uređaj).

•**Per-Device:** omogućava pristup serveru neograničenom broju korisnika sa onog uređaja kojem je dodeljena (User+Device zamena za Per-Seat).

•**Per-Server:** "stari" model licenciranja koji omogućava pristupanje, u istom trenutku, samo onoliko računara/korisnika koliko je licencirano

•**External Connector:** namenjen je za pristup spoljnih korisnika serveru. Kupljenom licencom neograničen broj odgovarajućih spoljnih korisnika može da pristupi jednoj kopiji servera. Ne podržava korišćenje hostinga.

•**Per-Processor:** Serveru može pristupati neograničen broj radnih stanica ali se mora kupiti onoliki broj procesorskih licenci koliko ima procesora u serverskom računaru. CAL-ovi nisu neophodni u ovoj implementaciji.

13.5 Vrste licenciranja

- **Retail:** Ove licence se kupuju *online* ili preko fizičke maloprodaje. Ovaj tip licenciranja se tipično koristi u malim organizacijama koje moraju da kupe ograničeni broj licenci.
- **OEM:** Ove licence se kupuju zajedno sa novim hardverom. Cena ovih licenci je tipično manja od maloprodajne, ali se ne mogu premeštati sa jednog računara na drugi.
- **Volume Licence:** Cena ovih licenci je tipično manja od cene u maloprodaji, ali je veća od OEM licenciranja. Neke *Volume Licensing* opcije dobijaju se na osnovu pretplate, a ne običnom kupovinom. Kupovinom ovih licenci dostupno je i osiguranje na softver. Ključna prednost volume licenciranja je pojednostavljenje procesa licenciranja.

Nezavisno od toga na koji način smo dobili naše serverske licence, imaćemo pravo da koristimo raniju verziju Windows-a.

Ovo se naziva Downgrade (pravo unazad) pravo.

13.5 – Podela softvera

- **Javno dostupan** (*public domain)* - softver sa kojim korisnik može raditi sve što želi: korišćenje,umnožavanje,distribucija, prodavanje bez dozvole
- **Softver sa otvorenim kodom** (*open source)*- besplatno se koristi, umnožava i distribuira, a dozvoljeno je i menjati izvorni kod i izmenjen softver dalje distribuirati ali pod istom licencom.
- **Besplatan softver** (*freevuare)*- besplatno je korišćenje i distribucija, ali se ne sme menjati. Taj softver se takođe izdaje pod posebnom licencom i definisanim pravilima korišćenja. Autor zadržava autorsko pravo.
- **Probni softver** (*shareware)*- sličan je besplatnom softveru, ali se u licencnom sporazumu obično traži da korisnik pošalje autoru određenu svotu novca nakon nekog određenog probnog peroda.
- **Komercijalni softver** (*commercial)*- ovaj softver korisnik mora da kupi da bi ga koristio, ali ne sme da ga kopira, distribuira ili menja. Postoje dva tipa komercijalnog softvera: softver koji korisnik može da kupi i licencirani softver. Ako korisnik kupi kopiju programa, može ga koristiti na način koji je definisan u zakonu o autorskim pravima. Danas je skoro sav softver licenciran i u tom slučaju korisnik kupuje samo licencu

Hvala na pažnji !!!

Pitanja

? ? ?