P12 Varnostno inženirstvo

1.1 Uvod

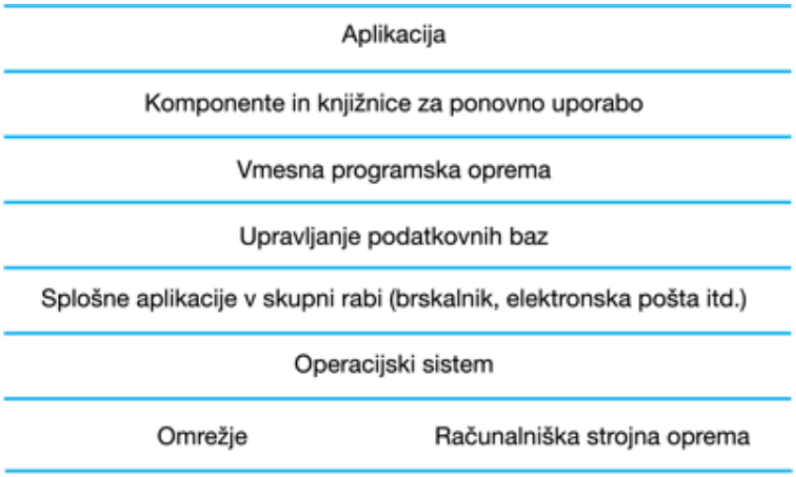
Varnostno inženirstvo predstavlja orodja, tehnike in metode za podporo razvoju in vzdrževanju sistemov, ki so odporni na zlonamerne napade.

1.1 Varnostne dimenzije

- **zaupnost** - *informacije v sistemu se lahko razkrijejo ali so na voljo uporabnikom oz. programom, ki nimajo dovoljenja za dostop do teh informacij*
- **neokrnjenost** - *če pride v sistemu do okvare informacij, to povzroči nezanesljivost informacij*
- **razpoložljivost** - *dostop do sistema ali njegovih podatkov, ki so običajno na voljo, ni mogoč*

1.2 Ravni varnosti

- **Varnost infrastrukture** zadeva ohranjanje varnosti vseh sistemov in omrežij, ki zagotavljajo infrastrukturo in množico skupnih storitev v okviru podjetja.
- **Varnost aplikacij** se ukvarja z varnostjo posameznih aplikacijskih sistemov ali sorodnih skupin .
- **Operativna varnost** se nanaša na varno delovanje in uporabo sistemov organizacije.



Slika 22.1: Sistemske ravni, kjer je lahko ogrožena varnost

Figure 1: Sistemske ravni, kjer je lahko ogoržena varnost

1.3 Varnost infrastrukture in aplikacij

Z **varnostjo aplikacij** se ukvarja **programsko inženirstvo**, kjer mora biti **sistem zasnovan** tako, da je odporen proti napadom.

Varnost infrastrukture je v domeni **upravljanja sistemov**, kjer je treba **infrastrukturo nastaviti** tako, da je odporna proti napadom.

1.4 Upravljanje varnosti sistema

Upravljanje varnosti sistema vsebuje številne aktivnosti:

- **upravljanje uporabnikov** in **dovoljenj**, kjer se dodaja in odstranjuje uporabnike iz sistema ter nastavlja ustrezna dovoljenja
- pri **uvajanju** in **vzdrževanju programske opreme** gre za nameščanje programske in vmesne programske opreme ter konfiguriranje teh sistemov, da se izognemo ranljivostim
- **nadzor napadov, odkrivanje** in **obnovitev** predstavlja spremljanje sistema proti nepooblaščenemu dostopu, oblikovanje strategij za odpornost do napadov in razvoj strategij za izdelavo varnostnih kopij in obnovitev

1.5 Operativna varnost

Uporabniki včasih izvajajo nevarna dejanja z namenom olajšanja svojega dela, zato vedno obstaja **kompromis** med **varnostjo** in **učinkovitostjo sistema**.

2 Varnost in zagotovljivost

2.1 Varnost

Varnost sistema je sistemska lastnost, ki odraža zmožnost sistema, da se zaščiti pred naključnim ali namernim zunanjim napadom.

2.2 Terminologija na področju varnostnega inženirstva

Tabela 22.1: Varnostna terminologija

Pojem	Opredelitev
sredstvo[104]	Nekaj vrednega, kar je treba zaščititi. Sredstvo je lahko sistem programske opreme ali podatki, ki jih ta sistem uporablja.
napad[105]	Izkoriščanje ranljivosti sistema. V splošnem prihaja od zunaj in poskuša namerno povzročiti škodo.
nadzor[106]	Zaščitni ukrep, ki zmanjša ranljivost sistema. Primer nadzora je šifriranje, ki zmanjša ranljivost šibkega sistema za nadzor dostopa.
izpostavljenost[107]	Potencialna izguba ali poškodba računalniškega sistema. Gre lahko za izgubo ali poškodbo podatkov in tudi izgubo časa ter truda, če je potrebna ponovna vzpostavitev po kršitvi varnosti.
grožnja[108]	Okoliščine, ki lahko povzročijo izgubo ali škodo. Lahko si jih predstavljamo kot sistemsko ranljivost, ki je izpostavljena napadu.
ranljivost[109]	Pomanjkljivost v računalniškem sistemu, ki se lahko izkoristi za povzročitev izgube ali škode.

Tabela 22.2 prikazuje primere posameznih terminov na problemski domeni Mentcare.

Tabela 22.2: Primeri terminov na problemski domeni Mentcare

Pojem	Opredelitev
sredstvo	Zdravstveni zapisi posameznega pacienta, ki prejema ali je prejel zdravljenje.
napad	Lažno predstavljanje pooblaščenega uporabnika.
nadzor	Sistem za preverjanje gesel onemogoča uporabniška gesla, ki so lastna imena ali besede, ki se pojavljajo v slovarju.
izpostavljenost	Finančna izguba pri potencialnih bolnikih, ki ne bodo poiskali zdravljenja, ker ne zaupajo kliniki glede varovanja osebnih podatkov. Finančna izguba zaradi sodnega postopka znane osebe. Izguba ugleda.
grožnja	Nepooblaščeni uporabnik pridobi dostop do sistema tako, da ugiba prijavne podatke (uporabniško ime in geslo) pooblaščenega uporabnika.
ranljivost	Sistem šibkih gesel z možnostjo uporabe preprostih gesel, ki jih je mogoče ugotoviti. Enolični identifikatorji uporabnikov, ki so enaki imenom uporabnikov.

Figure 2: Varnostna topologija

2.3 Primer nepooblaščenega dostopa do sistema Mentcare

- *Osebje klinike se v sistem Mentcare prijavlja z uporabniškim imenom in geslom. Sistem zahteva, da so gesla dolga vsaj 8 znakov, vendar dovoljuje nastavitev gesla brez nadaljnjega dodatnega preverjanja. Napadalec ugotovi, da se ena izmed znanih oseb zdravi zaradi težav z duševnim zdravjem. Pridobiti želi nezakonit dostop do informacij, s katerimi bi lahko nato izsiljeval to znano osebo.*
- *Medicinskemu osebju se napadalec predstavi kot zaskrbljen svojec. Med pogovorom poskuša pridobiti potrebne podatke za dostop tako, da opazuje oznake z imeni in išče dodatne podatke o družinskih članih medicinskega osebja. Ko ugotovi imena in priimke zaposlenih, poskuša z različnimi kombinacijami uporabniških imen in gesel (npr. imena, priimki, datumi, otroci ipd.) pridobiti dostop do sistema.*

2.4 Vrste groženj

- **grožnja prestrezanja** napadalcu omogoča dostop do sredstva
- **grožnja prekinitve** napadalcu omogoča, da povzroči nedostopnost dela sistema
- **grožnja spremembe** omogoča napadalcu spreminjanje sistemskega sredstva
- **grožnja vgradnje** napadalcu omogoča vstavljanje lažnih informacij v sistem

2.5 Zagotavljanje varnosti

- **Izogibanje ranljivostim** - *sistem je zasnovan tako, da se ranljivosti ne pojavijo.*
- **Odkrivanje in odstranjevanje napadov** - *sistem je zasnovan tako, da se napadi na ranljivosti odkrijejo in nevtralizirajo, preden povzročijo izpostavljenost.*
- **Omejitev izpostavljenosti in predelava** - *sistem je zasnovan tako, da so negativne posledice uspešnega napada čim manjše.*

2.6 Varnost in zagotovljivost

Zagotovljivost je lastnost sistema, da zagotovi svojo razpoložljivost, zanesljivost, zaščito, odpornost, celovitost in zmožnost vzdrževanja.

Varnost in razpoložljivost: Običajen napad na spletni sistem je napad z zavrnitvijo storitve, kjer je spletni strežnik preobremenjen z zahtevami za storitve iz različnih virov.

Varnost in zanesljivost: Če je sistem napaden in so sistema ali njegovi podatki poškodovani kot posledica tega napada, lahko to povzroči sistematske napake, ki ogrožajo zanesljivost sistema.

Varnost in zaščita: Če napad poškoduje sistem ali njegove podatke, pomeni, da prvotne predpostavke o varnosti morda ne držijo.

Varnost in odpornost: Odpornost je značilnost sistema, da se upre in ponovno vzpostavi po škodljivih dogodkih.

3 Varnost v podjetjih

3.1 Varnost je poslovno vprašanje

Varnost veliko stane in pomembno je, da se **varnostne odločitve** sprejemajo na **stroškovno učinkovit način**.

3.2 Organizacijske varnostne politike

Varnostne politike morajo določati splošne strategije dostopa do informacij, ki bi se morale uporabljati v celotni organizaciji.

3.3 Varnostne politike

Da je obvladovanje tveganja učinkovito, bi morale imeti organizacije **dokumentirano varnostno politiko**, ki določa:

- **sredstva, ki jih je treba zaščititi**
- **raven razščite, ki je potrebna za različne vrste sredstev**
- **odgovornost posameznih uporabnikov, upravljalcev in podjetja**
- **obstoječe varnostne postopke in tehnologije, ki jih je treba ohraniti**

3.4 Ocena in upravljanje varnostnih tveganj

Ocena in upravljanje tveganj se ukvarja z ocenjevanjem morebitnih izgub, ki bi lahko nastale zaradi napadov na sistem.

Upravljanje tveganj mora voditi organizacijska varnostna politika, kjer je vključeno:

- **predhodna** ocena tveganja
- ocena tveganja **v življenskem ciklu**
- ocena **operativnega** tveganja

3.4.1 Predhodna ocena tveganja

Cilj začetne ocene tveganja je opredelitev splošnih tveganj, ki so prisotna v sistemu, in se odločiti, ali je mogoče doseči ustrezno raven varnosti po razumni ceni.

3.4.2 Ocena tveganja pri načrtvoanju

Ta ocena tveganja poteka v življenskem ciklu razvoja sistema in temelji na načrtvoanju sistemov in odločitvah o implementaciji.

3.4.3 Ocena operativnega tveganja

Ta postopek ocene tveganja se osredotoča na uporabo sistema in možna tveganja, ki lahko nastanejo zaradi človeškega vedenja.

4 Varnostne zahteve

4.1 Varnostna specifikacija

Varnostna specifikacija ima nekaj skupnega s **specifikacijo zahtev za zaščito** - v obeh primerih se želimo izogniti slabim dogodkom.

4.2 Vrste varnostnih zahtev

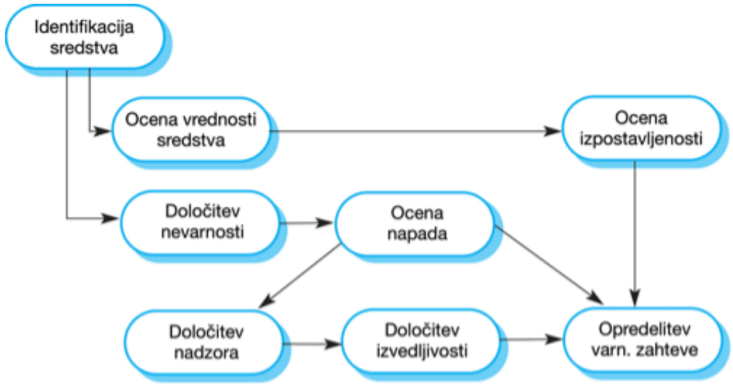
- zahteve za **identifikacijo** - *določajo, ali naj sistem identificira svoje uporabnike pred njihovo interakcijo s sistemom*
- zahteve za **preverjanje istovetnosti identitete** - *določajo, kako so uporabniki identificirani*
- zahteve za **avtorizacijo dostopa** - *določajo privilegije in dovoljenja za dostop identificiranih uporabnikov*
- zahteve **imunitete** - *določajo, kako naj se sistem ščiti pred virusi, črvi in podobnimi grožnjami*
- zahteve **integritete** - *določajo, kako se je mogoče izogniti okvari podatkov*
- zahteve **zaznavanja vdorov** - *določajo, katere mehanizme je treba uporabiti za odkrivanje napadov na sistem*

- zahteve za **preprečevanje zanikanja** - *določajo, da udeleženec v transakcji ne more zanikati svojega sodelovanja v tej transakcji*
- zahteve **zasebnosti** - *določajo, kako ohraniti zasebnost podatkov*
- zahteve za **varnostno revizijo** - *določajo prisotnost revizijske sledi in možnost preverjanja uporabe sistema*
- zahteve **sistemskega vzdrževanja** - *določajo, kako lahko aplikacija prepreči nenameren obhod varnostnih mehanizmov*

4.3 Klasifikacija varnostnih zahtev

- **zahteve izogibanja tveganj** - *določajo tveganja, ki se jim je treba izogniti*
- **zahteve ugotavljanja tveganj** - *opredeljujejo mehanizme, ki ob pojavitvi tveganja le tega identificarajo in tveganje nevtralizirajo*
- **zahteve zmanjševanja tveganja** - *določajo, kako naj bo sistem načrtovan, da je mogoča obnovitev sistemskih sredstev, potem, ko je že prišlo do izgube*

4.4 Ocena varnostnega tveganja



Slika 22.2: Predhodni postopek ocenjevanja tveganja varnostnih zahtev

Figure 3: Predhodni postopek ocenjevanja tveganja varnosntih zahtev

4.4.1 Ocena varnostnega tveganja sistema Mentcare

Tabela 22.3: Analiza sredstev v predhodni oceni tveganj za sistem Mentcare

Sredstvo	Vrednost	Izpostavljenost
Informacijski sistem	**Visoka.** Zahteva se za podporo vseh kliničnih posvetov. Potencialno kritičen za varnost.	**Visoka.** Finančna izguba v primeru zaprtja klinike. Stroški obnove sistema. Možne poškodbe bolnika, če zdravljenja ni mogoče predpisati.
Podatkovna baza bolnikov	**Visoka.** Zahteva se za podporo vseh kliničnih posvetov. Potencialno kritična za varnost.	**Visoka.** Finančne izgube v primeru zaprtja klinike. Stroški obnove sistema. Možne poškodbe bolnika, če zdravljenja ni mogoče predpisati.
Posamezen bolniški zapis	**Običajno nizka**, čeprav je lahko visoka pri določenih bolj izpostavljenih bolnikih.	**Nizka neposredna izguba**, vendar možna izguba ugleda.

Tabela 22.4 prikazuje nekatere grožnje, s katerimi se lahko sistem Mentcare sooča.

Tabela 22.4: Analiza groženj in nadzora v predhodni oceni tveganj za sistem Mentcare

Grožnja	Verjetnost	Nadzor	Izvedljivost
Nepooblaščeni uporabnik pridobi upraviteljski dostop in onemogoči dostop do sistema.	Nizka	Upravljanje sistema je dovoljeno zgolj z določenih lokacij, ki so fizično varne.	Nizki stroški izvedbe, vendar je treba paziti na distribucijo dostopnih ključev in zagotoviti, da so le-ti na voljo v nujnih primerih.
Nepooblaščen uporabnik pridobi dostop sistemskega uporabnika in dostopa do zaupnih informacij.	Visoka	Od vseh uporabnikov se zahteva, da se overijo z uporabo biometričnega mehanizma. Vse spremembe informacij o bolniku so zabeležene, da je omogočeno sledenje uporabi sistema.	Tehnično izvedljivo, vendar cenovno neugodna rešitev. Možen odpor uporabnika. Preprosto in pregledno za implementacijo, podpira tudi obnovitev.

Varnostne zahteve sistema Mentcare:

- Informacije o bolniku se na začetku klinične obravnave prenesejo na varno območje na odjemalcu, ki ga uporablja klinično osebje.
- Vse informacije o bolniku na odjemalcu morajo biti šifrirane.
- Podatki o bolniku se po končani klinični obravnavi naložijo v podatkovno bazo in se izbrišejo iz odjemalčevega računalnika.
- Vzdrževati je treba dnevnik vseh sprememb sistemske podatkovne baze, ki se nahaja na ločenem računalniku od strežnika podatkovne baze.

4.5 Primeri zlorab

Primeri zlorab:

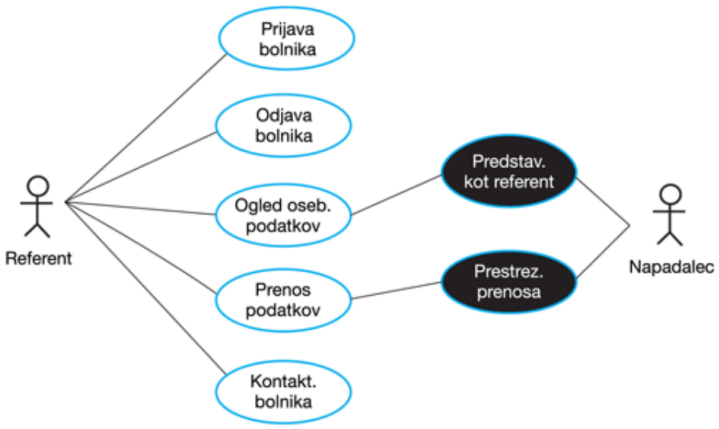
- grožnja prestrezanja
- grožnja prekinitve
- grožnja spremembe
- grožnja vgradnje

4.5.1 Primeri zlorab v sistemu Mentcare

5 Varna zasnova sistema

Pomembna sta dva vidika zasnove sistema:

- **zasnova arhitekture**



Slika 22.3: Primeri zlorab

Tabela 22.5: Primer uporabe **Prenos podatkov** v sistemu Mentcare

Naziv	Opis
Akter	Referent, sistem evidence bolnikov.
Opis	Referent lahko prenese podatke iz sistema Mentcare v splošno zbirko podatkov o bolnikih, ki jo vzdržuje zdravstveni organ. Preneseni podatki so lahko posodobljeni osebni podatki (npr. naslov, telefonska številka itd.) ali povzetek bolnikove diagnoze in zdravljenja.
Podatki	Osebni podatki bolnika, povzetek zdravljenja.
Vhod	Ukaz, ki ga zahteva referent.
Izhod	Potrditev, da je sistem evidence bolnikov posodobljen.
Komentarji	Referent mora imeti ustrezna varnostna dovoljenja za dostop do informacij o bolnikih in sistema evidence bolnikov.

Primere zlorab lahko opišemo na več načinov, kjer je pogost način dodatek opisa primerov uporabe (glej tabelo 22.5), kar prikazuje tabela 22.6.

Tabela 22.6: Primer uporabe **Prestrezanje prenosa** v sistemu Mentcare **(primer zlorabe)**

Naziv	Opis
Akter	Referent, sistem evidence bolnikov, napadalec.
Opis	Referent prenese podatke iz svojega računalnika v sistem Mentcare na strežniku. Napadalec prestreže prenos podatkov in si prisvoji kopijo teh podatkov.
Podatki (sredstva)	Osebni podatki bolnika, povzetek zdravljenja.
Napad	V omrežje je nameščen sistem za spremljanje omrežnega prometa, ki prestreže podatkovne pakete med računalnikom referenta in strežnikom. Med računalnikom referenta in strežnikom se vzpostavi lažni posredniški strežnik, ki prepriča odjemalca, da le-ta komunicira neposredno s strežnikom.
Preprečevanje	Vsa omrežna oprema mora biti vzdrževana v zaklenjenem prostoru. Vzdrževalci, ki dostopajo do opreme, morajo biti akreditirani. Vsi prenosi podatkov med odjemalcem in strežnikom morajo biti šifrirani. Komunikacija med odjemalcem in strežnikom naj uporablja certifikat.
Zahteve	Vsa komunikacija med odjemalcem in strežnikom mora uporabiti zaščitno plast SSL. Protokol HTTPS uporablja preverjanje istovetnosti identitete in šifriranje na podlagi certifikatov.

Figure 4: Primeri zlorab

- **dobra praska**

5.1 Kompromisi pri načrtovanju

Zmogljivost: dodatni varnostni pregledi upočasnijo delovanje sistema.

Uporabnost: varnostni ukrepi lahko od uporabnikov zahtevajo, da si zapomnijo informacije ali zahtevajo dodatno interackijo za dokončanje transakcije.

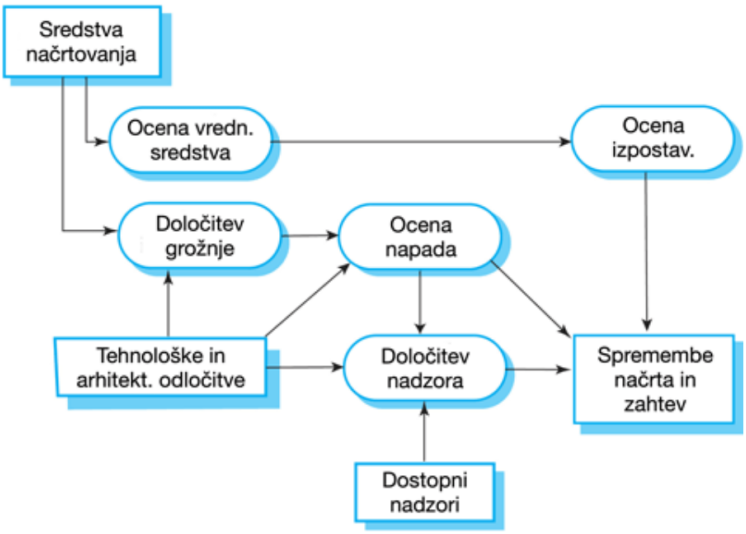
5.2 Ocena tveganja pri načrtvoanju

Proces načrtovanja sistema in ocena načrtovalskih tveganj sta medsebojno prepletena.

Slika 22.4: Načrtovanje in ocena tveganja

Figure 5: Načrtovanje in ocena tveganja

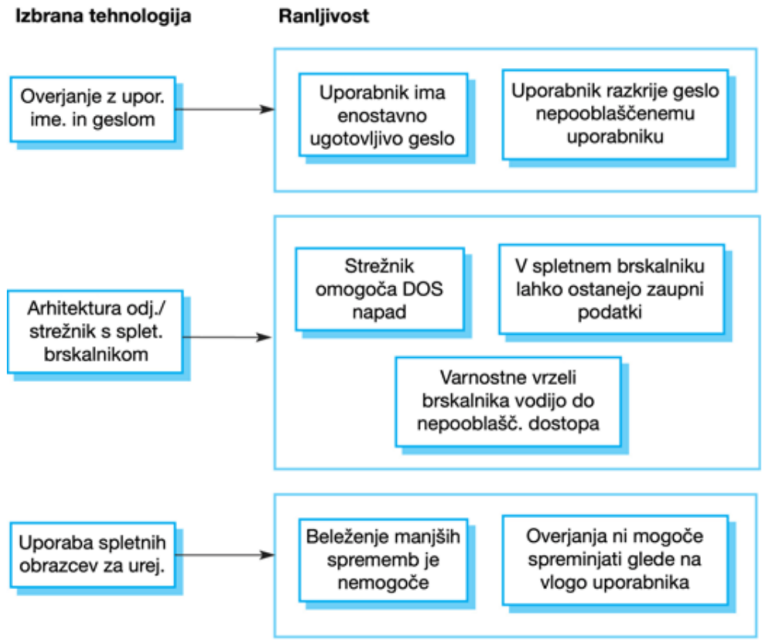
Na stopnji načrtovanja imamo informacije o predstavitvi in porazdelitvi informacij ter organizaciji podatkovne baze za zaščito sredstev na visoki ravni.



Slika 22.5: Ocena tveganja pri načrtovanju

Figure 6: Ocena tveganja pri načrtovanju

5.3 Načrtovalske odločitve pri uporabi COTS sistema pri implementaciji Mentcare



Slika 22.6: Ranljivosti, povezane z izbrano tehnologijo

Figure 7: Ranljivosti, povezane z izbrano tehnologijo

5.4 Zasnova arhitekture

Upoštevamo dva vidika:

- **zaščita** - *kako organizirati sistem, da bodo kritična sredstva zaščitena pred zunanjimi napadi*
- **porazdelitev** - *kako so sistemska sredstva porazdeljena, da so učinki uspešnega napada čim manjši*

5.4.1 Zaščita

Smiselna vpeljava **večplastne arhitekture**.

5.4.2 Porazdelitev

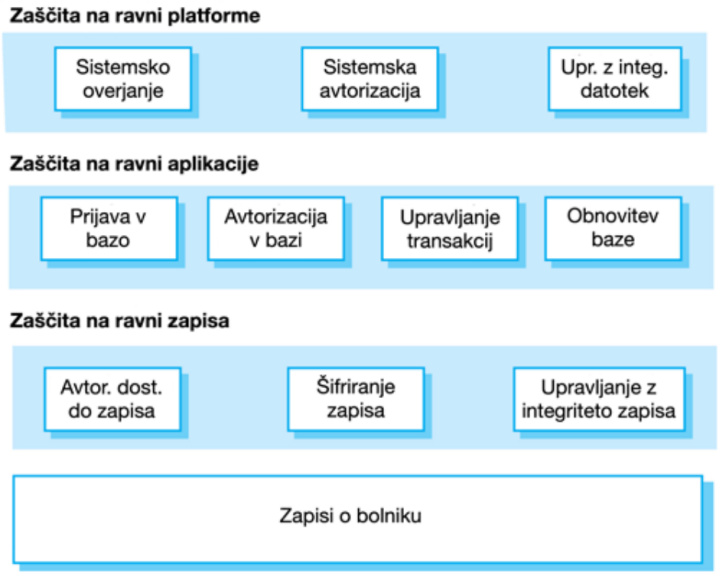
Porazdelitev sistemskih sredstev pomeni, da napadi na en sistem ne vodijo nujno k popolnemu nedelovanju sistemskih storitev.

5.5 Načrtovalske smernice za varnostno inženirstvo

6 Implementacija varnih sistemov

Pri implementaciji sta pomembna 2 vidika:

- **ranljivosti so pogosto značilne za izbran programski jezik**
- **varnostne ranljivosti so tesno povezane z zanesljivostjo programa**



Slika 22.7: Večplastna arhitektura zaščite

Figure 8: Večplastna arhitektura zaščite

Tabela 22.7: Varnostne smernice

Smernica	Opis
Varnostne odločitve naj temeljijo na opredeljeni varnostni politiki.	Opredeljena naj bo varnostna politika podjetja, ki določa temeljne varnostne zahteve, ki bi morale veljati za vse sisteme v podjetju. Težava je lahko v tem, da številna podjetja nimajo opredeljene varnostne politike.
Izogibajte se enotni točki odpovedi.	Zagotovite, da lahko do varnostne težave pride le, če je napaka prisotna pri več varnostnih postopkih. Npr. uporaba večstopenjskega preverjanja, kjer je poleg gesla prisotno še vprašanje o osebnih podatkih.
Napake naj bodo varne.	Če pride do odpovedi sistema, je treba zagotoviti, da nepooblaščeni uporabniki ne morejo dostopati do občutljivih podatkov kljub odsotnosti običajnih varnostnih postopkov.
Uravnotežite varnost in uporabnost.	Izogibajte se varnostnim postopkom, zaradi katerih je sistem težko uporabljati. Včasih morate sprejeti šibkejšo varnost, da bo sistem bolj uporaben.
Beležite uporabniške akcije.	Vzdržujte dnevnik uporabniških akcij, ki jih lahko analizirate, da ugotovite, kdo je izvedel katero akcijo. Če uporabniki vedo, da takšen dnevnik obstaja, je manj verjetno, da se bodo obnašali neodgovorno.
Uporabljajte redundanco in raznolikost.	Hranite več kopij podatkov in uporabite raznoliko infrastrukturo, tako da infrastrukturna ranljivost ne more biti edina točka odpovedi.
Določite format vseh vhodov sistema.	Če so znani vhodni formati, lahko preverite, ali so vsi vhodi v zahtevani obliki, tako da nepričakovani vnosi ne povzročajo težav.
Porazdelite sredstva.	Organizirajte sistem tako, da so sredstva na ločenih področjih in da imajo uporabniki dostop le do informacij, ki jih potrebujejo, in ne do vseh sistemskih informacij.
Načrtujte uvedbo sistema.	Načrtovanje sistema naj bo izvedeno tako, da se izognete težavam pri uvajanju.
Načrtujte za dosego obnovljivosti.	Sistem naj bo zasnovan tako, da je proces ponovne postavitve sistema ob uspešnem napadu poenostavljen.

Figure 9: Varnostne smernice

6.1 Programske smernice za večjo zanesljivost sistema

1. omejite vidnost informacij v programu
2. preverite veljavnost vseh vnosov
3. obravnavajte vse izjeme
4. zmanjšajte uporabo konkstruktov, ki so nagnjeni k napakam
5. zagotovite možnost ponovnega zagona
6. preverite meje seznamov
7. pri klicih zunanjih komponent vključite časovne omejitve
8. poimenujte konstante, ki predstavljajo dejanske vrednosti

7 Testiranje in zagotavljanje varnosti

Testiranje varnosti je testiranje obsega, do katerega se lahko sistem zaščiti pred napadi.

7.1 Vrednotenje varnosti

- **testiranje na podlagi izkušenj**
- **testiranje vdora**
- **analiza na podlagi orodja**
- **formalno vrednotenje**

8 Zaključne ugotovitve

- **Varnostno inženirstvo** se ukvarja z razvojem sistemov, ki so odporni proti zlonamernim napadom.
- **Varnostne grožnje** so lahko grožnje zaupnosti, neokrnjenosti in razpoložljivosti sistema ali njegovih podatkov.
- **Obvladovanje varnostnih tveganj** se ukvarja z ocenjevanjem morebitnih izgub zaradi napadov in odvisnimi varnostnimi zahtevami za zmanjšanje izgub.
- Za **določitev varnostnih zahtev** je treba določiti sredstva, potrebna zaščite, in opredeliti način zaščite teh sredstev z uporabo varnostnih tehnik in tehnologij.
- Pri oblikovanju **varne arhitekture** je ključna organizacija strukture sistema, kjer se ključna sredstva zaščitijo in porazdelijo, da se zmanjša izguba v primeru uspešnega napada.
- **Varnostne smernice** načrtovalce sistemov opomnijo na varnostna vprašanja, ki jih morda niso upoštevali pri prvotni zasnovi. Zagotavljajo osnovo za izdelavo varnostnih kontrolnih seznamov.
- **Vrednotenje varnost**i sistema je težavno, ker varnostne zahteve navajajo, kaj se v sistemu ne sme zgoditi in ne kaj bi se moralo. Poleg tega so napadalci inteligentni in imajo lahko več časa za iskanje slabosti, kot ga je na voljo za varnostno testiranje.