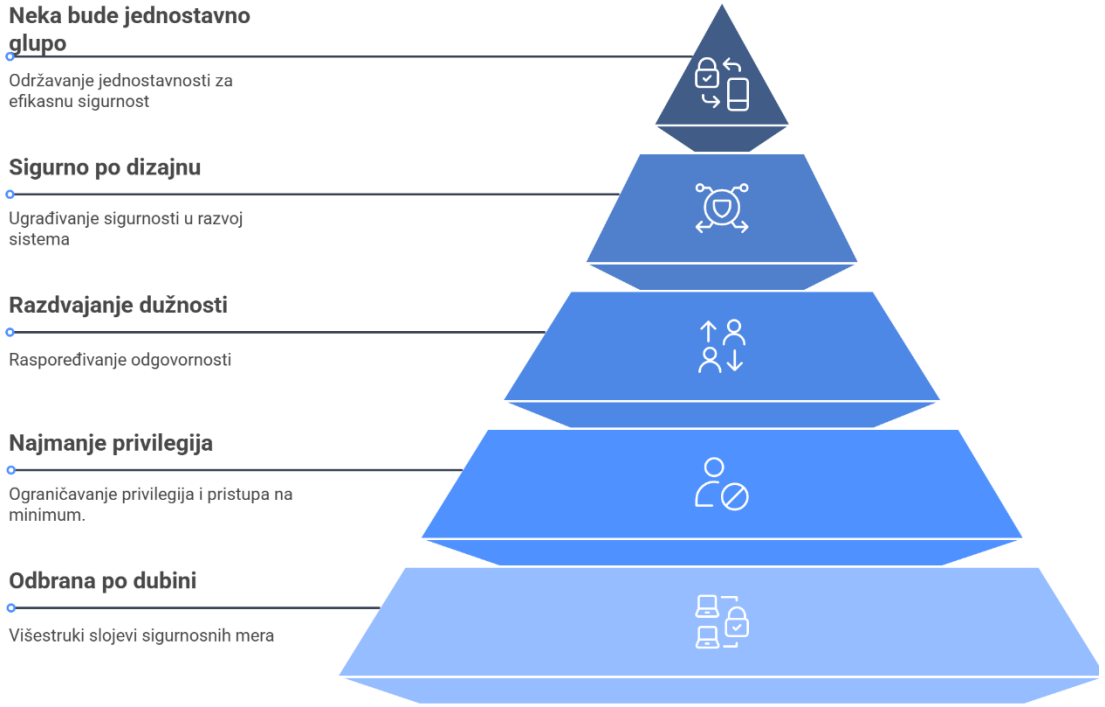
CYBER BEZBEDNOST ARHITEKTURA

Predavač: dr Dušan Stefanović

OSNOVE CYBER SECURITY ARHITEKTURE

Bezbedonosni principi su sastavni deo cyber security arhitekture koji nas štite od širokog spektra pretnji

Pet Bezbedonosnih principa koje treba obavezno implementirati

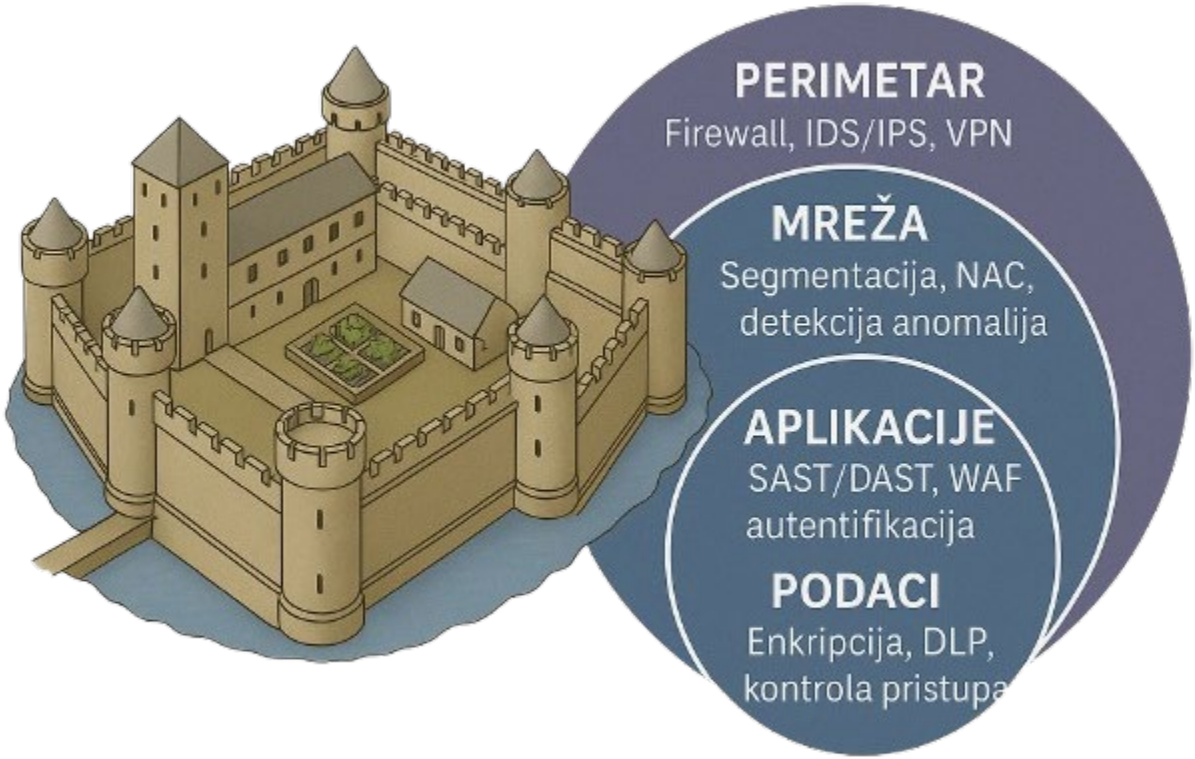


PRINCIP ODBRANE PO DUBINI

Odbrana po dubini je strategija koja podrazumeva implementaciju višestrukih slojeva sigurnosnih kontrola kako bi se zaštitili od različitih potencijalnih pretnji.

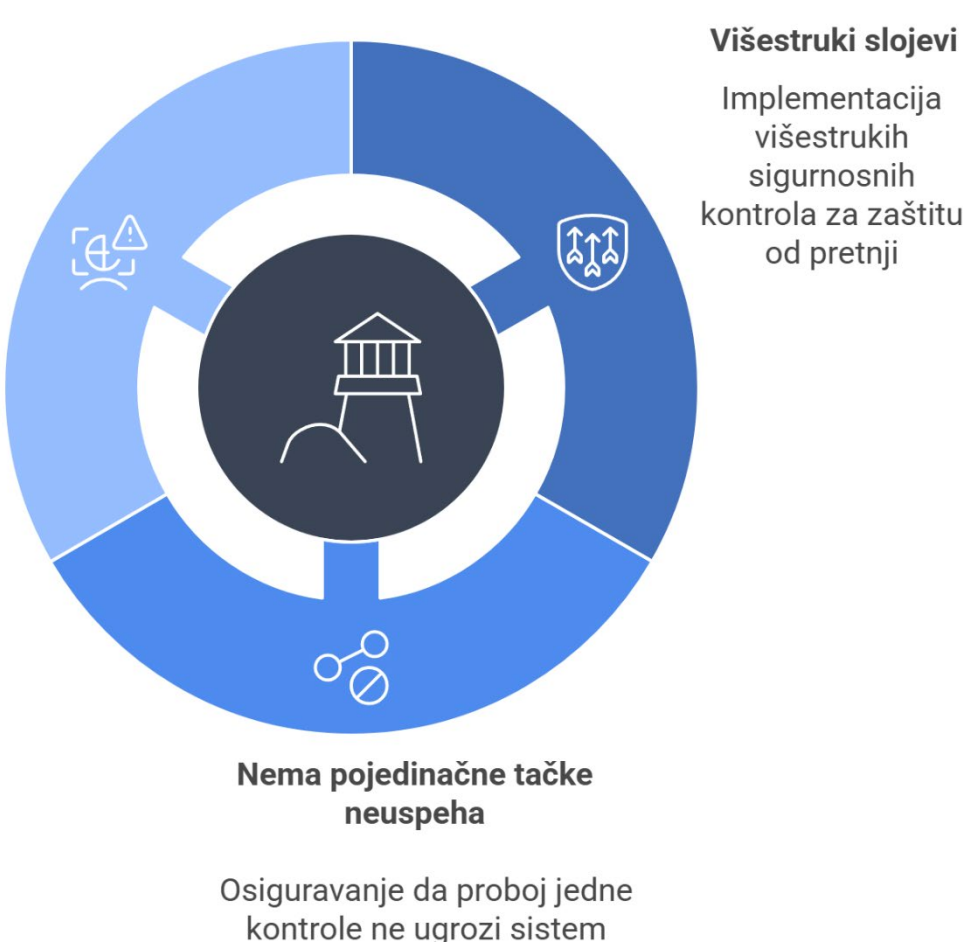
Proboj jedne sigurnosne kontrole ne znači da je sistem kao celina ugrožen

Sistem je dizajniran da ne postoji ***Single Point of Failure***.

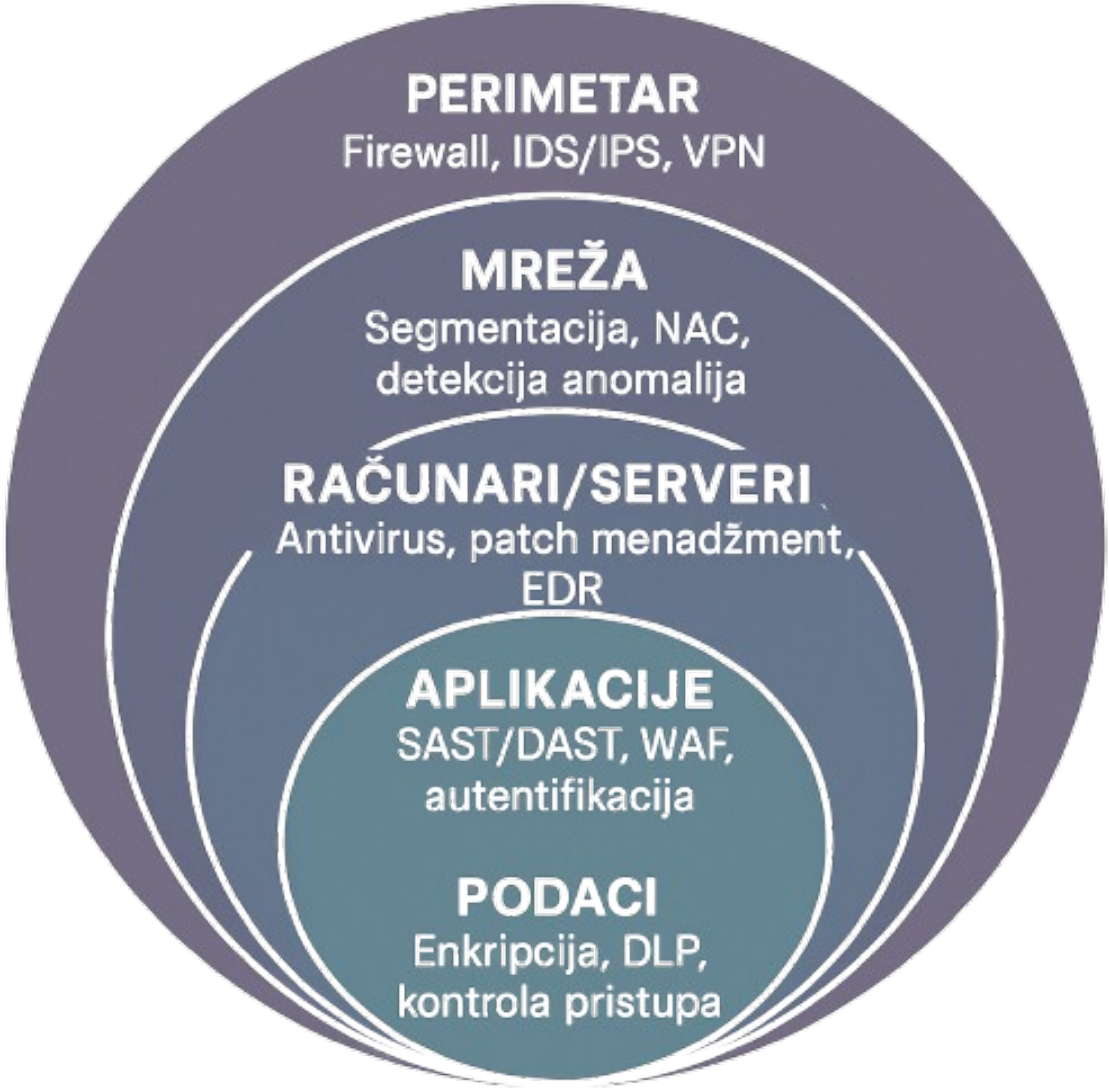


STRATEGIJA ODBRANE PO DUBINI

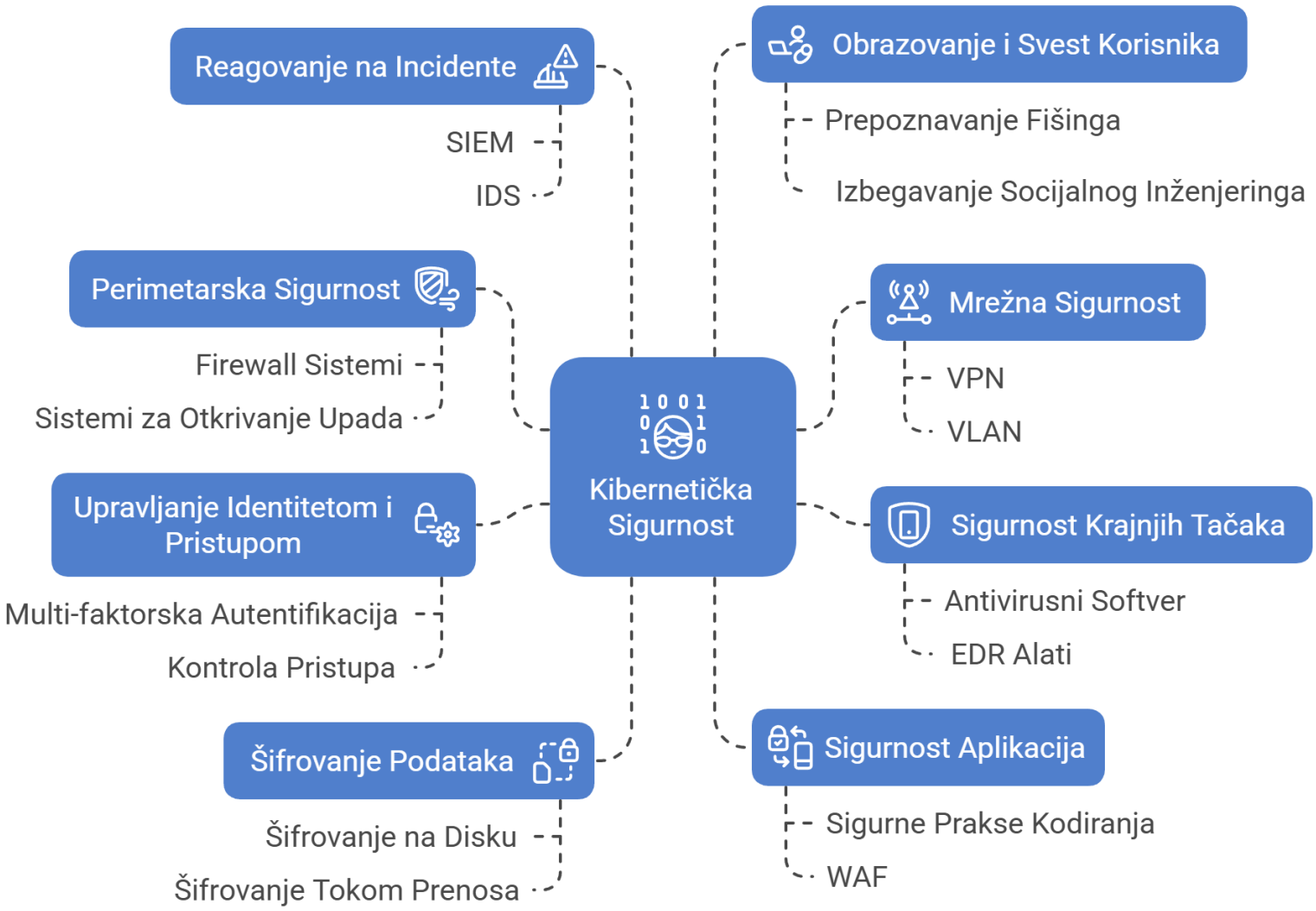
Koncept se zasniva na ideji da nijedna pojedinačna sigurnosna mera ne može pružiti potpunu zaštitu, iz tog razloga su potrebni višestruki slojevi odbrane kako bi se rizici efikasno umanjili.



STRATEGIJA ODBRANE PO DUBINI



KOMPONENTE ODBRANE PO DUBINI



1.Perimetarska sigurnost:Zaštita od spoljnjih pretnji (firewall sistemi i sistemima za otkrivanje i sprečavanje upada)

2.Mrežna sigurnost: Segmentacija i zoniranje se koriste kako bi se razdvojili različiti delovi mreže i ograničio pristup na osnovu principa najmanjih privilegija(VPN, VLAN, kontrola pristupa mreži i praćenje mrežnog saobraćaja)

3.Sigurnost krajnjih tačaka: Zaštita pojedinačnih uređaja poput računara, pametnih telefona i tableta sa antivirusnim softverom I alatima za otkrivanje i reagovanje na pretnje (EDR) i host-based firewall-ovima kako bi se sprečile infekcije malverom i neovlašćen pristup.

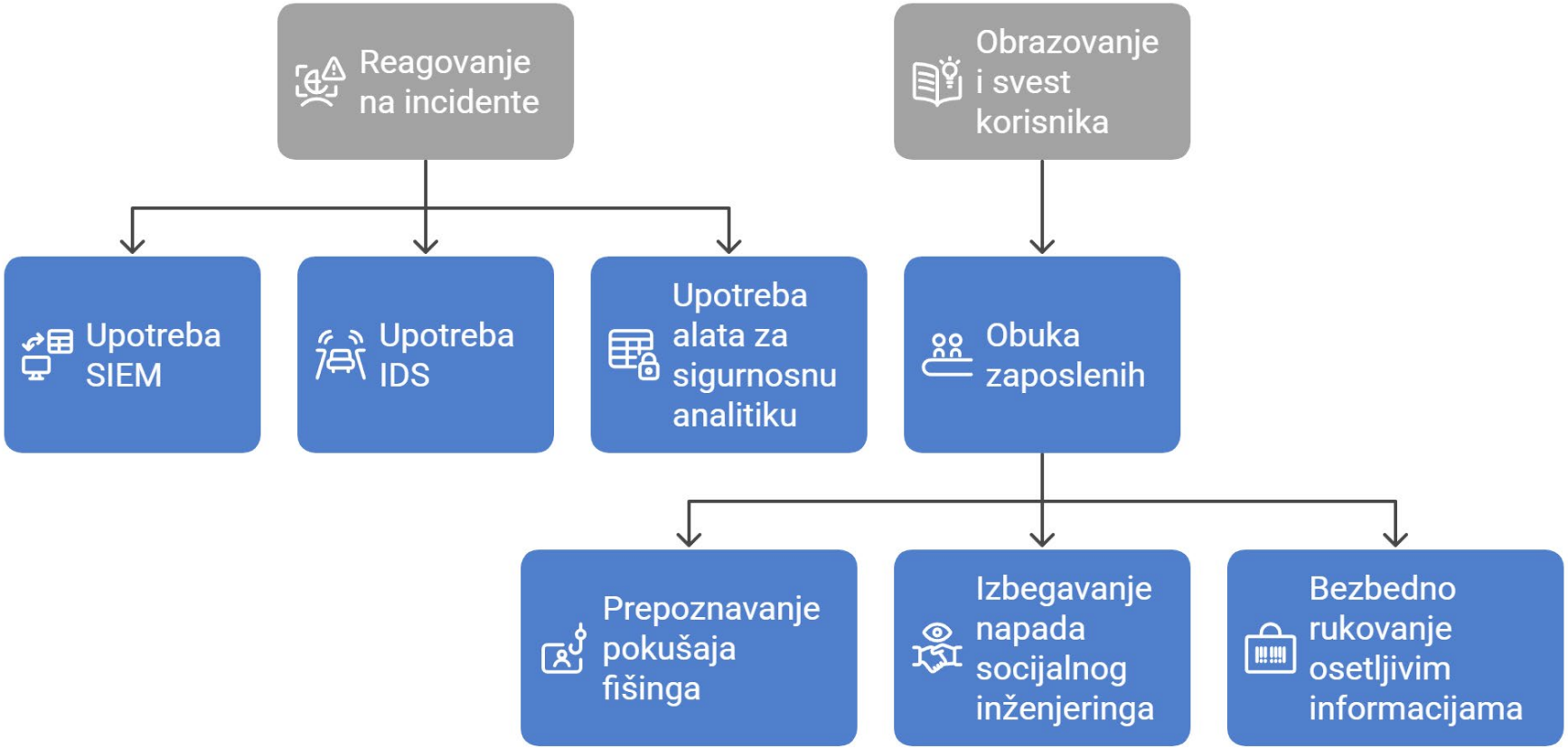
4. Upravljanje identitetom i pristupom (IAM): Implementacija snažnih mehanizama autentifikacije poput multi-faktorske autentifikacije (MFA) i sprovođenje stroge kontrole pristupa kako bi se osiguralo da samo ovlašćeni korisnici imaju pristup resursima.

5. Šifrovanje podataka: Šifrovanje osetljivih podataka na disku i tokom prenosa kako bi se sprečio neovlašćen pristup čak i ako budu presretnuti ili ukradeni.

6. Sigurnost aplikacija: Osiguravanje aplikacija putem sigurnih praksi kodiranja, redovnih procena ranjivosti i firewall-ova za veb aplikacije (WAF) kako bi se zaštitili od uobičajenih veb napada.

7. Reagovanje na incidente: Upotreba sistema za upravljanje informacijama i događajima o sigurnosti (SIEM), sistema za otkrivanje upada (IDS) i alata za sigurnosnu analitiku kako bi se pratila mrežna aktivnost i otkrivali nepravilnosti ili potencijalni sigurnosni prekidi.

8. Obrazovanje i svest korisnika: Obuka zaposlenih, kao što su prepoznavanje pokušaja fišinga, izbegavanje napada socijalnog inženjeringa i bezbedno rukovanje osetljivim informacijama.



Fizička bezbednost

Sprečava fizički pristup uređajima i serverima

Politike, procedure i svest

Obuhvata ljudski faktor kroz obuku i politike

Perimetar

Štiti ulazne tačke između mreža

Interna mreža

Štiti internu komunikaciju unutar organizacije

Host

Bezbednost pojedinačnih računara i servera

Aplikacije

Kontroliše pristup aplikacijama i proverava identitet

Podaci

Štiti informacije kao najvredniji resurs

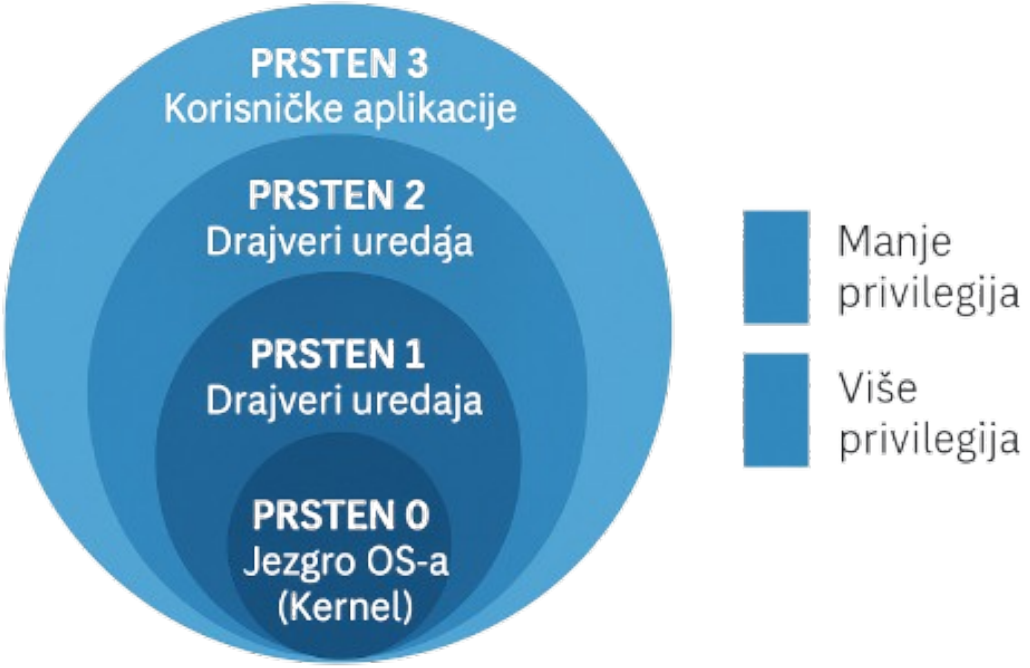
PRINCIP NAJMANJIH PRIVILEGIJA

Korisnici mogu da dobiju samo onoliko privilegija i pristupa resursima koji su im neophodni da izvrše zadatak

Ovaj princip ima za cilj minimiziranje potencijalnih rizika i smanjenje površine napada

Ograničavanje privilegija smanjuje potencijalne rizike od neovlašćenog pristupa, zloupotrebe privilegija i širenja štetnog softvera.

Implementacija principa najmanjih privilegija često zahteva saradnju između timova za informacionu tehnologiju (IT) i poslovnih korisnika, kako bi se razumele potrebe korisnika i efikasno upravljalo privilegijama.



STRATEGIJA NAJMANJIH PRIVILEGIJA

4 **Smanjenje površine napada**

Smanjuje potencijalne ulazne tačke za sajber napade.

3 **Minimiziranje rizika**

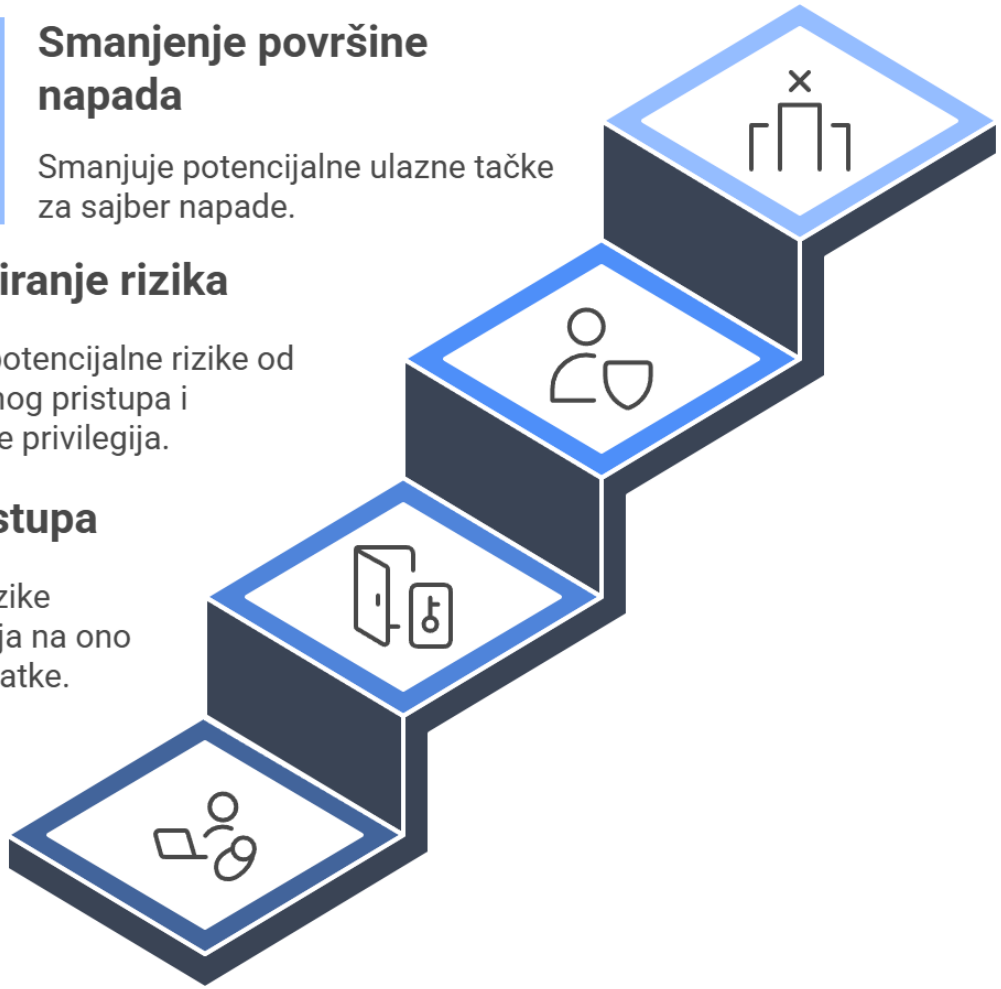
Smanjuje potencijalne rizike od neovlašćenog pristupa i zloupotrebe privilegija.

2 **Ograničavanje pristupa**

Smanjuje potencijalne rizike ograničavanjem privilegija na ono što je neophodno za zadatke.

1 **Razumevanje potreba korisnika**

Uključuje saradnju između IT i poslovnih korisnika kako bi se identifikovale neophodne privilegije.



ZERO TRUST SECURITY MODEL

Model "Zero Trust" (Nulto poverenje) je pristup koji pretpostavlja da se ni jedan entitet ili proces ne sme automatski smatrati pouzdanim, čak ni ako se nalazi unutar interne mreže organizacije.

Ovaj model zahteva kontinuiranu verifikaciju i proveru identiteta i dozvola za pristup resursima, bez obzira na to da li se korisnik ili resurs nalaze unutar ili izvan zaštićene mreže.

ZERO TRUST SECURITY MODEL

Zero Trust (Never trust, always verify**)**

svaki zahtev proverava:

a) ko si

b) odakle si

c) sa kog uređaja

d) šta tražiš

KLJUČNE KOMPONENTE ZERO TRUST MODELA

1. 👨‍💼 **Users (Korisnici)**
   → Identitet korisnika mora biti jasno potvrđen (autentikacija, MFA).

2. 💻 **Devices (Uređaji)**
   → Proverava se zdravstveno stanje, bezbednosni status i integritet uređaja.

3. 🌐 **Network Traffic (Mrežni saobraćaj)**
   → Kontrola i inspekcija mrežnog saobraćaja (mikrosegmentacija, detekcija anomalija).

4. 🧠 **Applications (Aplikacije)**
   → Pristup aplikacijama se dozvoljava po principu najmanjih privilegija.

5. 📁 **Data (Podaci)**
   → Pristup podacima je strogo kontrolisan, uz praćenje aktivnosti i zaštitu enkripcijom

ZERO TRUST SECURITY MODEL

Glavne komponente Zero Trust modela uključuju:

1.Kontinuiranu verifikaciju identiteta: Zahteva stalno proveravanje identiteta korisnika i uređaja koji pristupaju mreži ili resursima. Ovo može uključivati korišćenje višestrukog faktorskog autentifikacije (MFA) i biometrijske autentifikacije.

2.Granularne dozvole za pristup: Umesto široko definisanih privilegija, Zero Trust model promoviše davanje korisnicima samo onoliko privilegija koliko im je potrebno da obave svoje zadatke (princip najmanjih privilegija).

3.Mikrosegmentacija mreže: Mreža se deli na male segmente kako bi se ograničio protok podataka i smanjila površina napada. Svaki segment se tretira kao nezavisna zona sa svojim pravilima pristupa i sigurnosnim kontrolama.

4.Sigurnosni nadzor i analiza: Kontinuirano praćenje mrežnog saobraćaja i analiza aktivnosti kako bi se otkrile neobične ili sumnjive aktivnosti koji mogu ukazivati na napad ili zloupotrebu.

5.Nulta pretpostavka: Umesto pretpostavke da su entiteti unutar mreže pouzdani, Zero Trust model pretpostavlja da niko i ništa nije automatski pouzdano, pa se svaki zahtev za pristup pažljivo verifikuje.

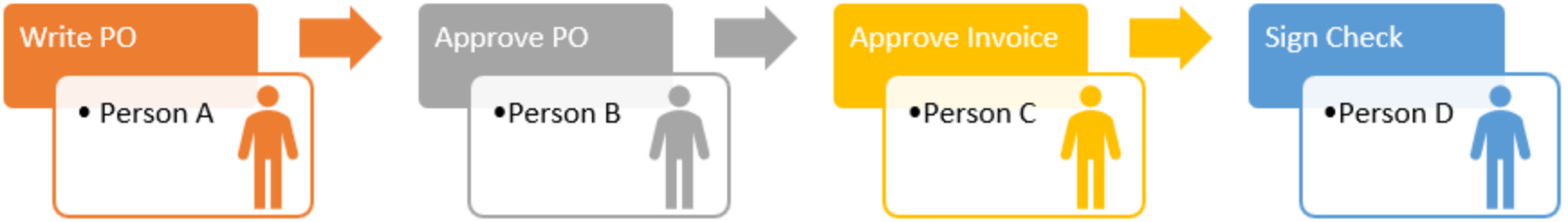
PRINCIP RAZDVAJANJA DUŽNOSTI

Razdvajanje dužnosti je koncept raspodele odgovornosti i prava pristupa tako da nijedan pojedinac ili entitet ne može imati apsolutnu kontrolu nad kritičnim sistemima i procesima.

Ovaj princip ima za cilj smanjenje rizika od zloupotrebe ovlašćenja, grešaka i prevara.

Izbegava se na ovaj način ***Single Point of Control***

Osoba koja je zadužena za unos podataka ne bi trebalo da bude ista osoba koja odobrava ili proverava te podatke.



kreiranje narudžbenice | odobrenje | odobrenje fakture | potpis / isplata

BEZ RAZDVAJANJA DUŽNOSTI

Jedna osoba radi sve:

a) napiše narudžbenicu

b) odobri je

c) odobri fakturu

d) izvrši plaćanje

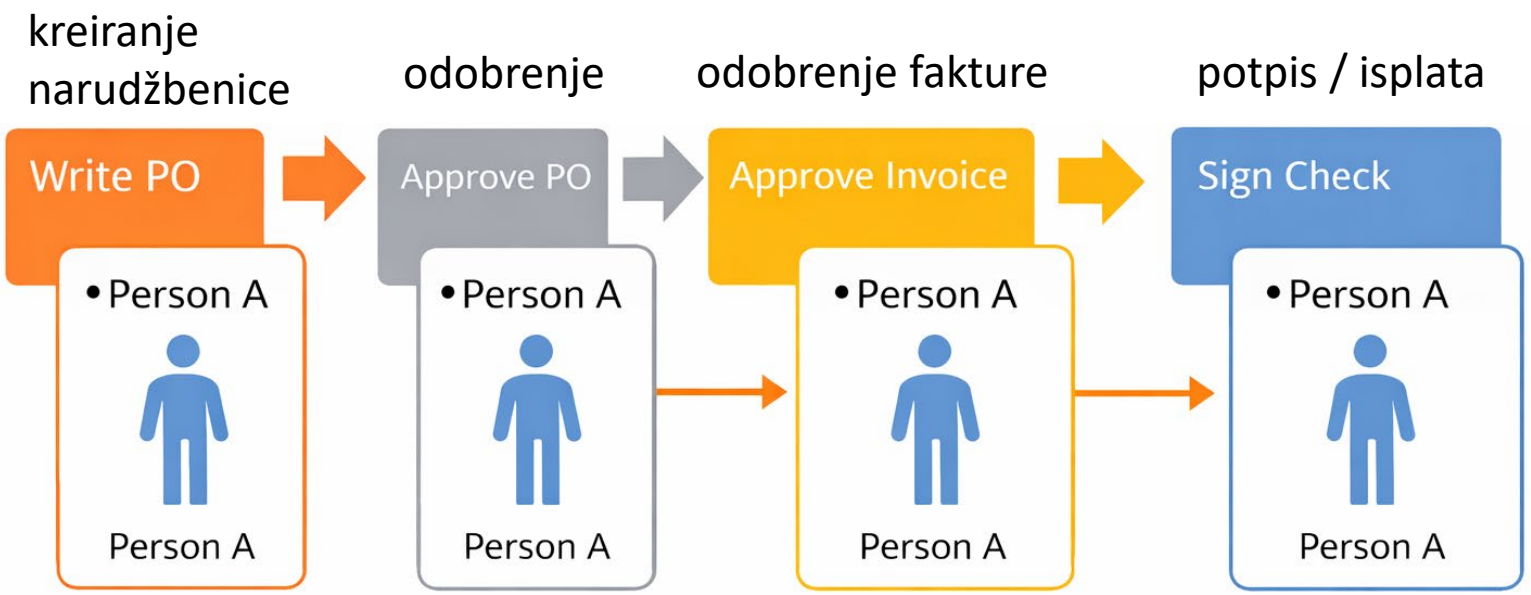
Može da:

a) izmisli trošak

b) uplati sebi novac

c) sakrije tragove

❌ TOTALNI RIZIK

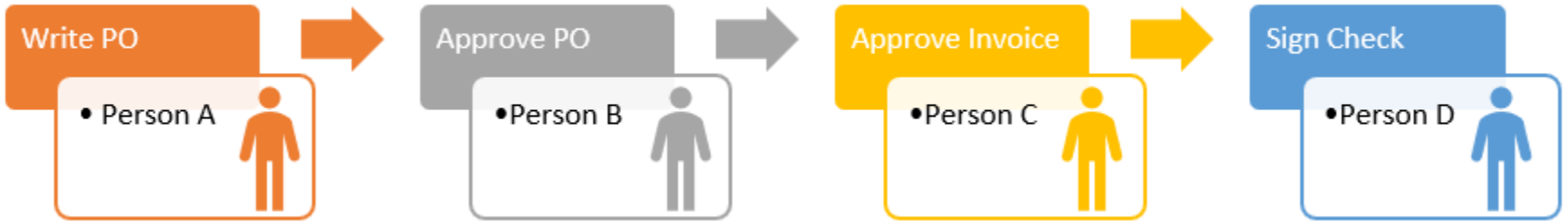


PRINCIP RAZDVAJANJA DUŽNOSTI

Svaki korak radi **druga osoba**

NIKO nema potpunu kontrolu nad celim procesom

Mnogo je teže za zloupotrebu jer napadač mora da kompromituje više osoba



kreiranje narudžbenice odobrenje odobrenje fakture potpis / isplata

podržava Zero Trust:

a) ne veruje se jednoj osobi
b) svaka akcija mora biti proverena

PRINCIP RAZDVAJANJA DUŽNOSTI

Primena razdvajanja dužnosti može pomoći organizacijama da postignu nekoliko ciljeva u vezi sa sigurnošću i integritetom podataka:

Smanjenje rizika od grešaka

Deljenje odgovornosti smanjuje verovatnoću grešaka i propusta.

Smanjenje rizika od zloupotrebe privilegija

Ograničavanje ovlašćenja sprečava zloupotrebu pristupa.

Osiguranje integriteta podataka

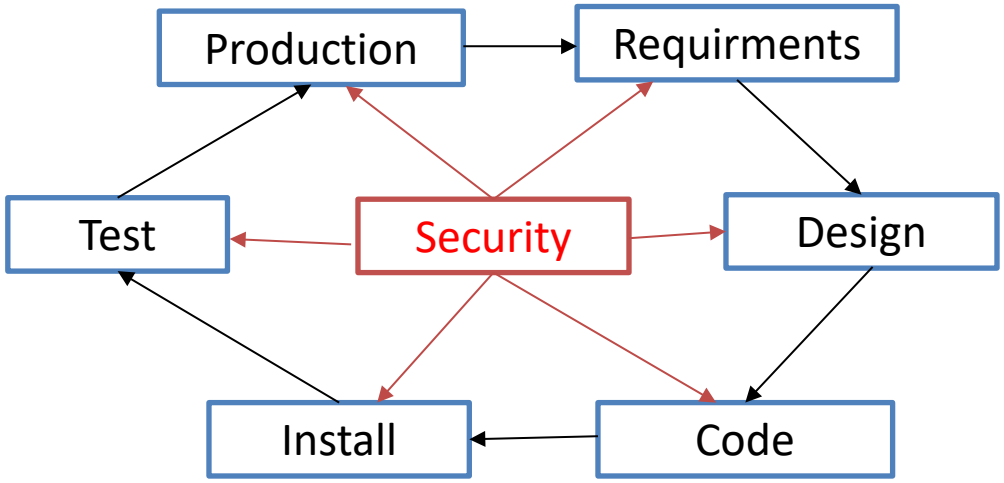
Održavanje tačnosti i pouzdanosti podataka.

Usklađenost sa regulativama

Ispunjenje zakonskih zahteva i standarda.

PRINCIP SECURE BY DESIGN

Secure by design princip je pristup razvoju softvera i sistema koji se fokusira na integraciji bezbednosnih principa i praksi tokom svih faza razvoja proizvoda, umesto dodavanja sigurnosnih mera nakon što je proizvod već razvijen.



PRINCIP KEEP IT SIMPLE STUPID

Keep it simple, stupid (KISS) je princip dizajna koji promoviše ideju da kompleksnost treba svesti na minimum kako bi se olakšalo razumevanje, upotreba i održavanje proizvoda ili sistema.

Kompleksnost i sigurnost ne idu zajedno

PITANJE 1

Koji od sledećih principa NIJE među pet osnovnih bezbednosnih principa u okviru cyber security arhitekture?

A) Princip najmanjih privilegija

B) Secure by Design

C) Razdvajanje dužnosti

D) Brzina razvoja sistema

PITANJE 2

Šta predstavlja strategija „odbrane po dubini“?

A) Korišćenje više slojeva sigurnosnih kontrola za umanjenje rizika

B) Implementacija samo jednog jakog sigurnosnog sloja

C) Brisanje podataka nakon svake sesije

D) Upotreba fizičkih prepreka u sistemima

PITANJE 3

Šta predstavlja heuristička analiza u antivirusnim alatima?

A) Analizu istorije korisničkog ponašanja

B) Otkrivanje poznatih pretnji putem potpisa

C) Otkrivanje novih pretnji analizom sumnjivog ponašanja fajlova

D) Korišćenje ručne provere svakog fajla od strane administratora

PITANJE 4

Koja tvrdnja NAJBOLJE opisuje Zero Trust model?

A) Korisnici imaju punu slobodu unutar internog sistema

B) Potrebna je verifikacija samo kod prvog pristupa

C) Nijedan entitet se ne smatra pouzdanim bez stalne provere

D) Svi korisnici unutar mreže se automatski smatraju pouzdanim

PITANJE 5

Šta je glavni cilj razdvajanja dužnosti (Separation of Duties)?

A) Olakšavanje zaposlenima da rade više poslova

B) Smanjenje rizika od zloupotreba i grešaka

C) Povećanje broja zaposlenih u IT sektoru

D) Automatizacija svih bezbednosnih funkcija