CYBER SECURITY ARHITEKTURA

Predmet: Zaštita podataka u komunikacionim mrežama

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

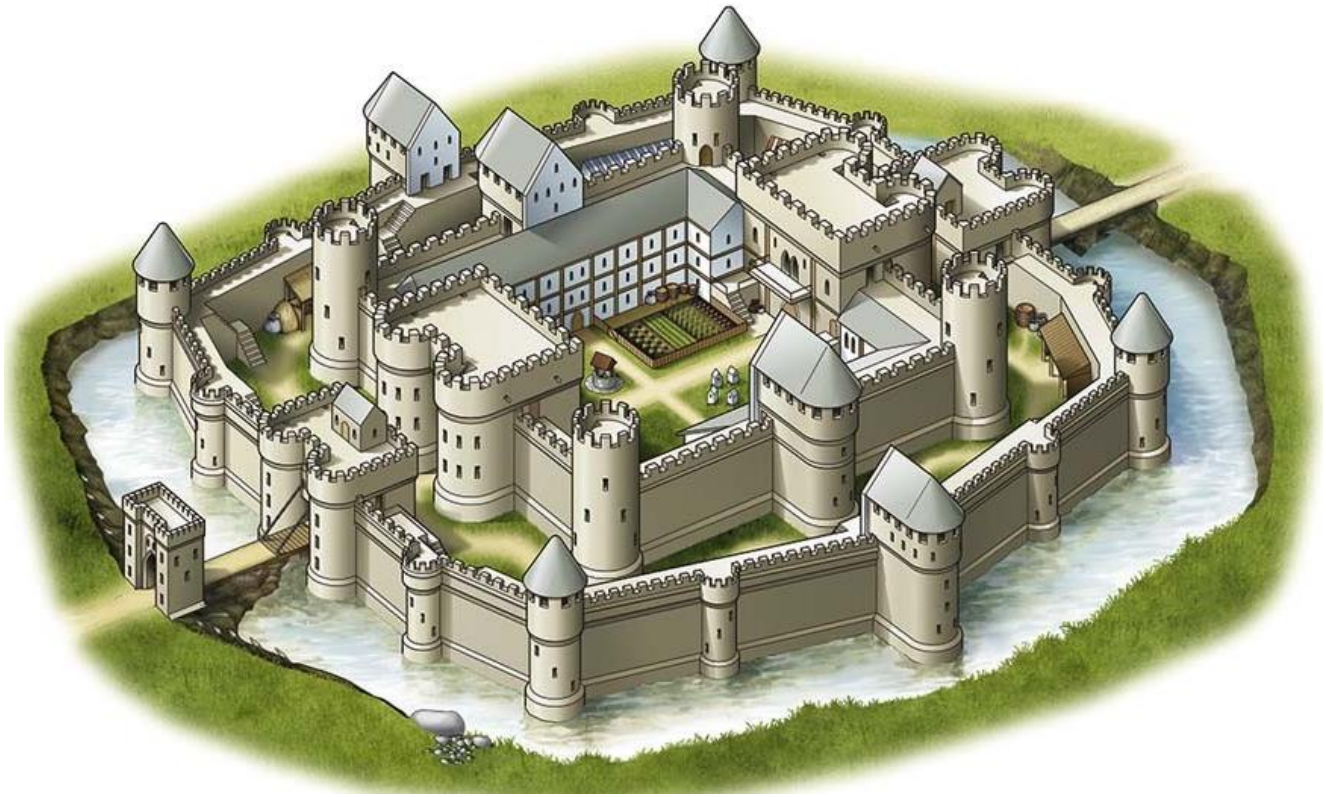
1. Princip odbrane po dubini (defense in depth)
2. Princip najmanjih privilegija (least privilege)
3. Princip razdvajanja dužnosti (separation of duties)
4. Princip Secure by design
5. Princip keep it simple stupid

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***.

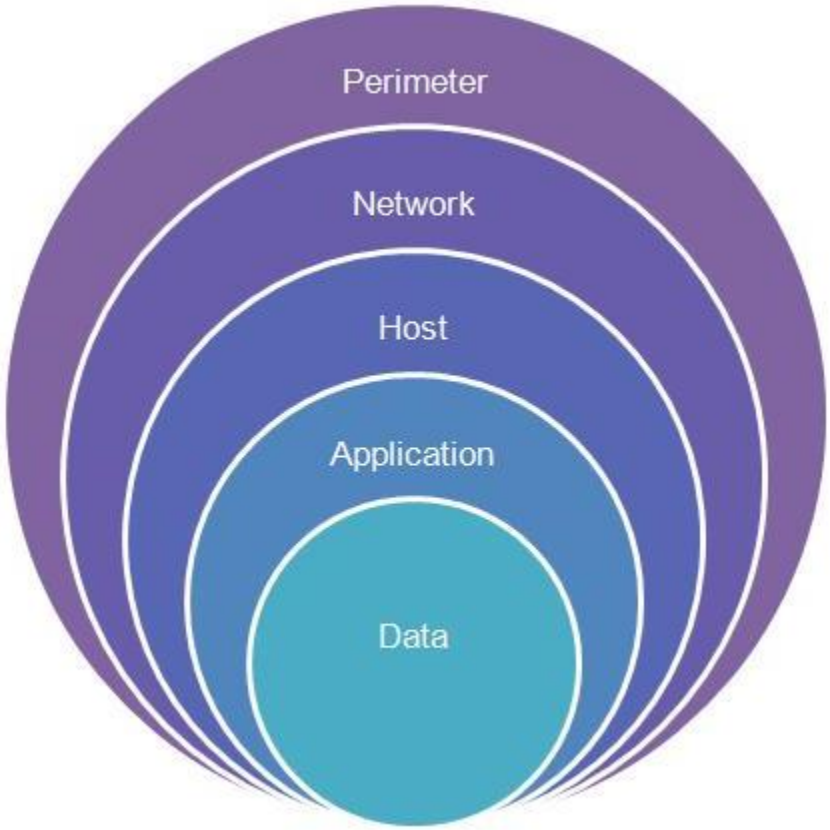


PRINCIP ODBRANE PO DUBINI

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.

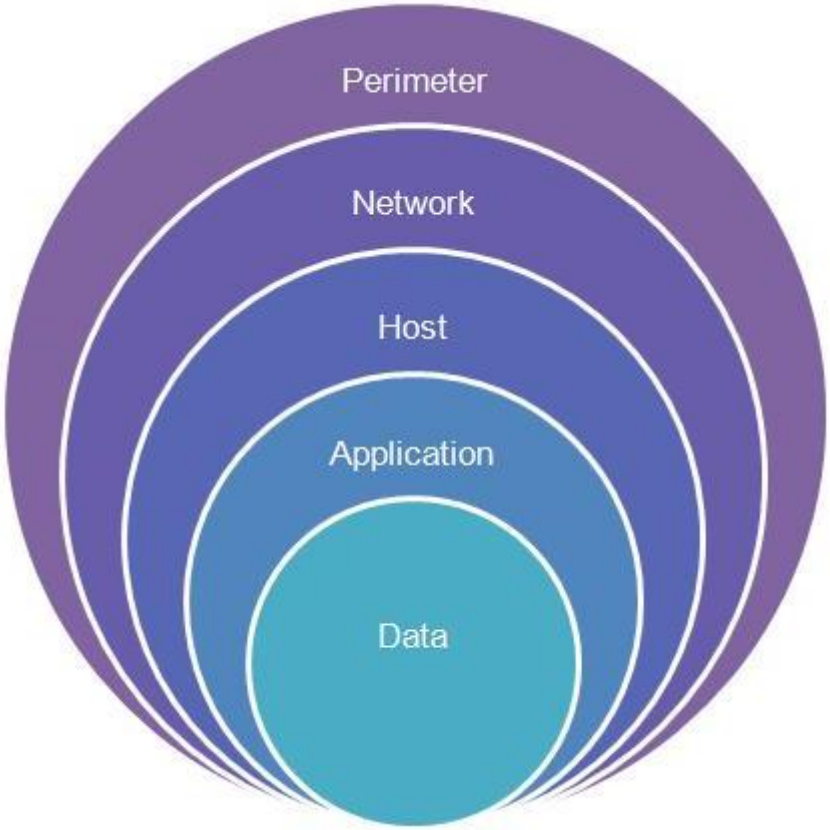


PRINCIP ODBRANE PO DUBINI

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.

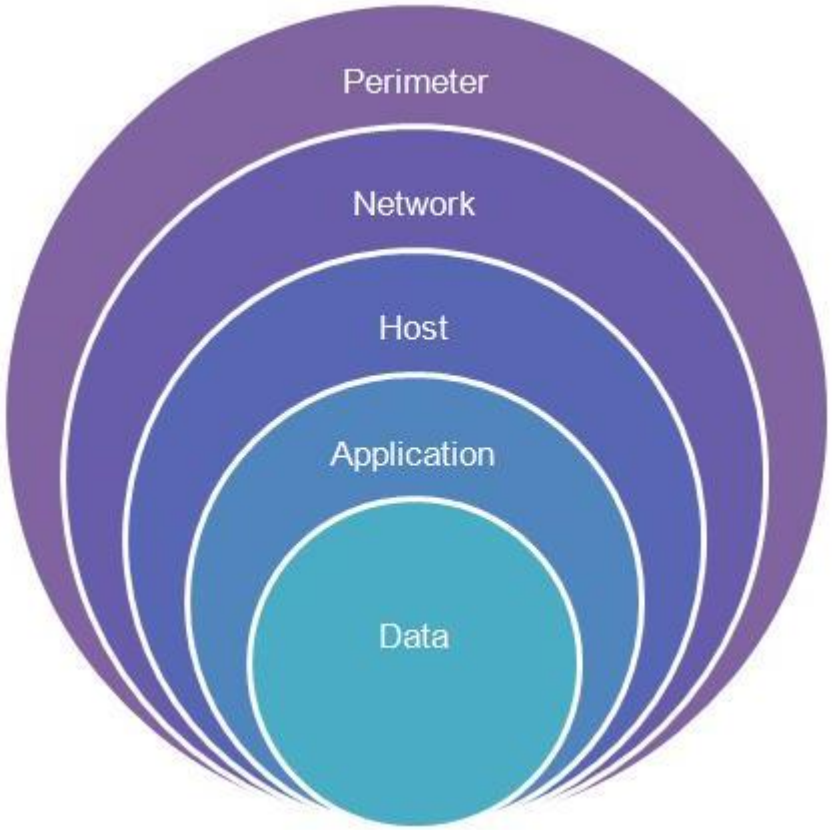
6. Sigurnost aplikacija: Osiguravanje aplikacija putem sigurnih praksi kodiranja, redovnih procena ranjivosti i firewall-ova za veb aplikacije (WAF) kako bi se zaštitili od uobičajenih veb napada.

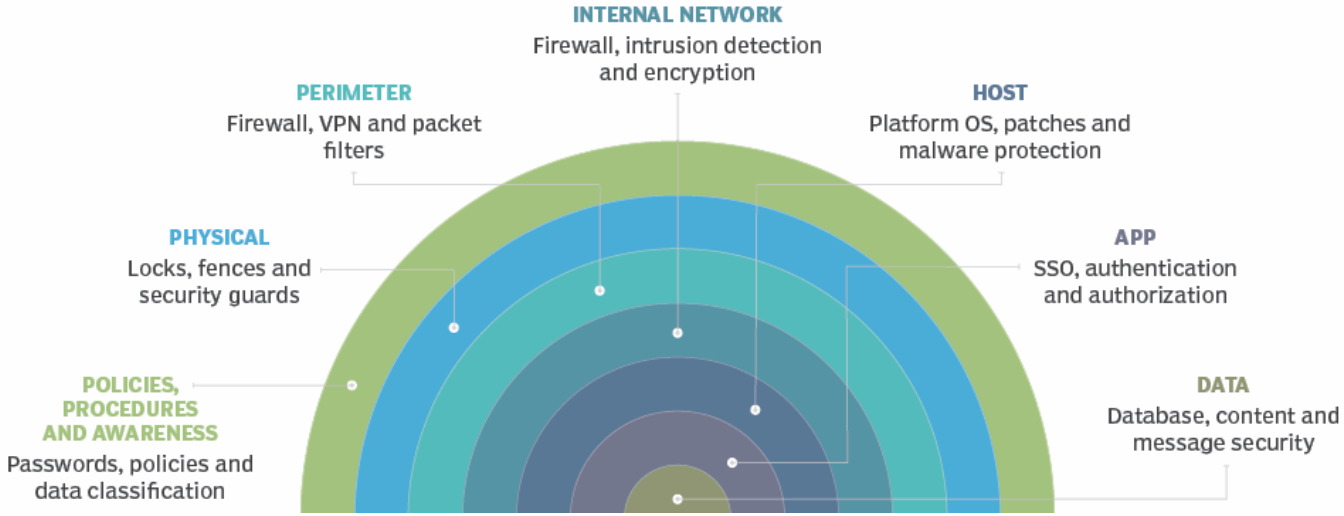


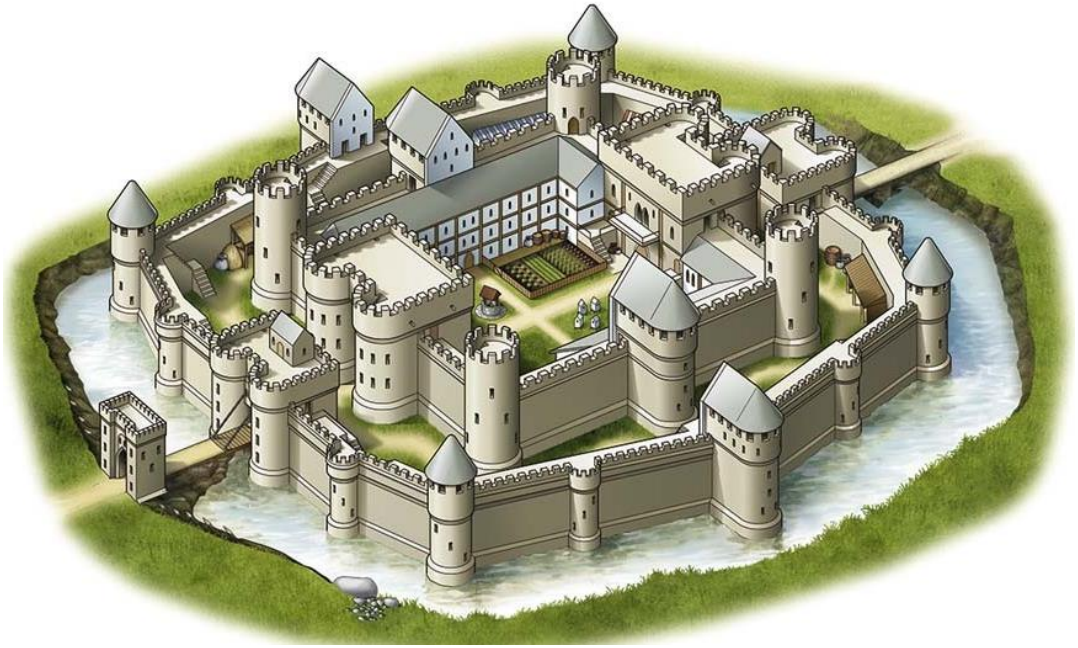
PRINCIP ODBRANE PO DUBINI

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.




INTERNAL NETWORK
Firewall, intrusion detection and encryption
PERIMETER
Firewall, VPN and packet filters
HOST
Platform OS, patches and malware protection
PHYSICAL
Locks, fences and security guards
APP
SSO, authentication and authorization
POLICIES, PROCEDURES AND AWARENESS
Passwords, policies and data classification
DATA
Database, content and message security



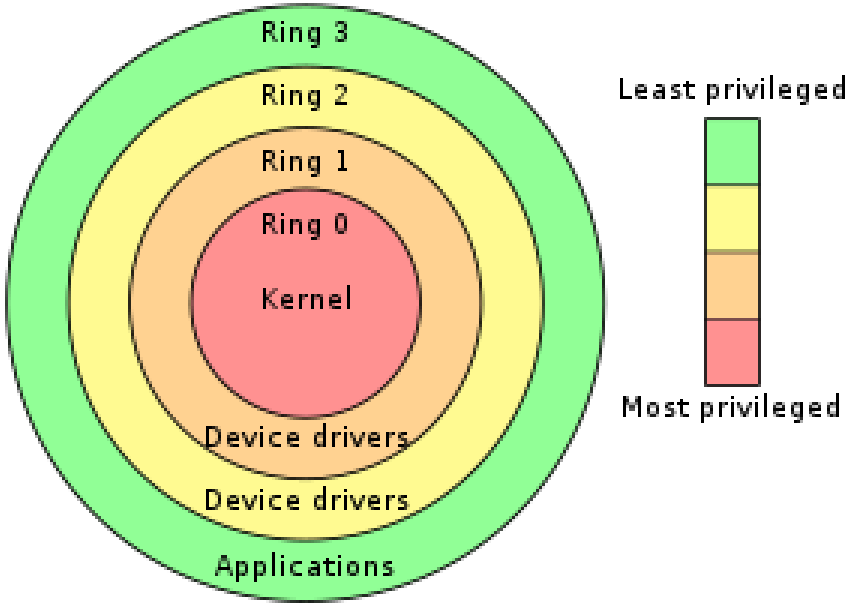
PRINCIP NAJMANJIH PRIVILEGIJA

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.

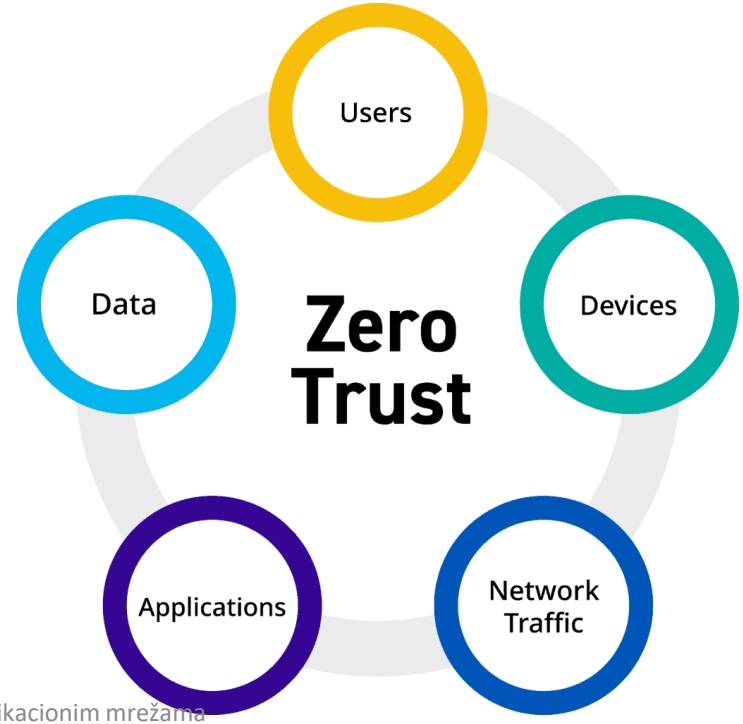
Implementacija principa najmanjih privilegija često zahteva saradnju između timova za informacionu tehnologiju (IT) i poslovnih korisnika, kako bi se razumele potrebe korisnika i efikasno upravljalo privilegijama.



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

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.

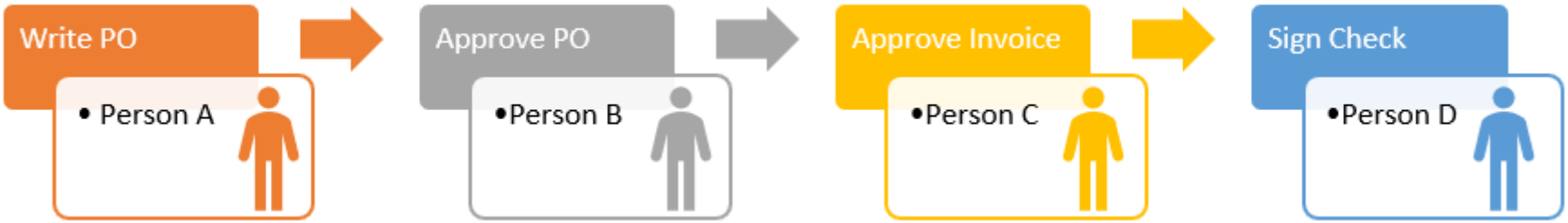
PRINCIP RAZDVAJANJA DUŽNOSTI

Razdvajanje dužnosti je koncept raspodeljivanja 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



PRINCIP RAZDVAJANJA DUŽNOSTI

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

1.Smanjenje rizika od grešaka: Deljenje odgovornosti između više pojedinaca ili timova može smanjiti verovatnoću grešaka ili propusta koji mogu dovesti do nepredviđenih problema ili gubitka podataka.

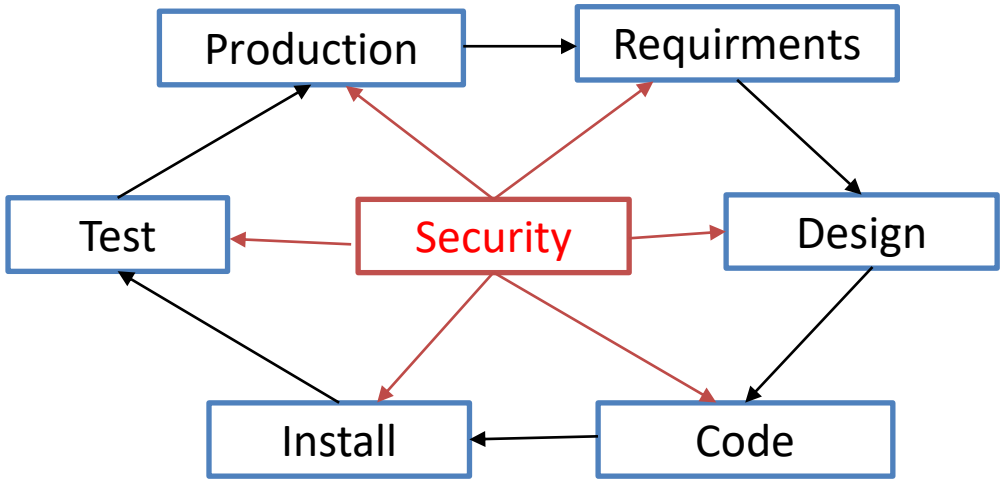
2.Smanjenje rizika od zloupotrebe privilegija: Razdvajanje dužnosti ograničava mogućnost pojedinca da zloupotrebi svoje ovlašćenje ili pristup kritičnim resursima.

3.Osiguranje integriteta podataka: Ovaj princip može pomoći u očuvanju integriteta podataka tako što sprečava neovlašćene promene ili manipulacije.

4.Usklađenost sa regulativama: Mnoge regulative, kao što su Sarbanes-Oxley Act (SOX) i General Data Protection Regulation (GDPR), zahtevaju primenu razdvajanja dužnosti kao deo standarda i procedura zaštite podataka.

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