Uvod

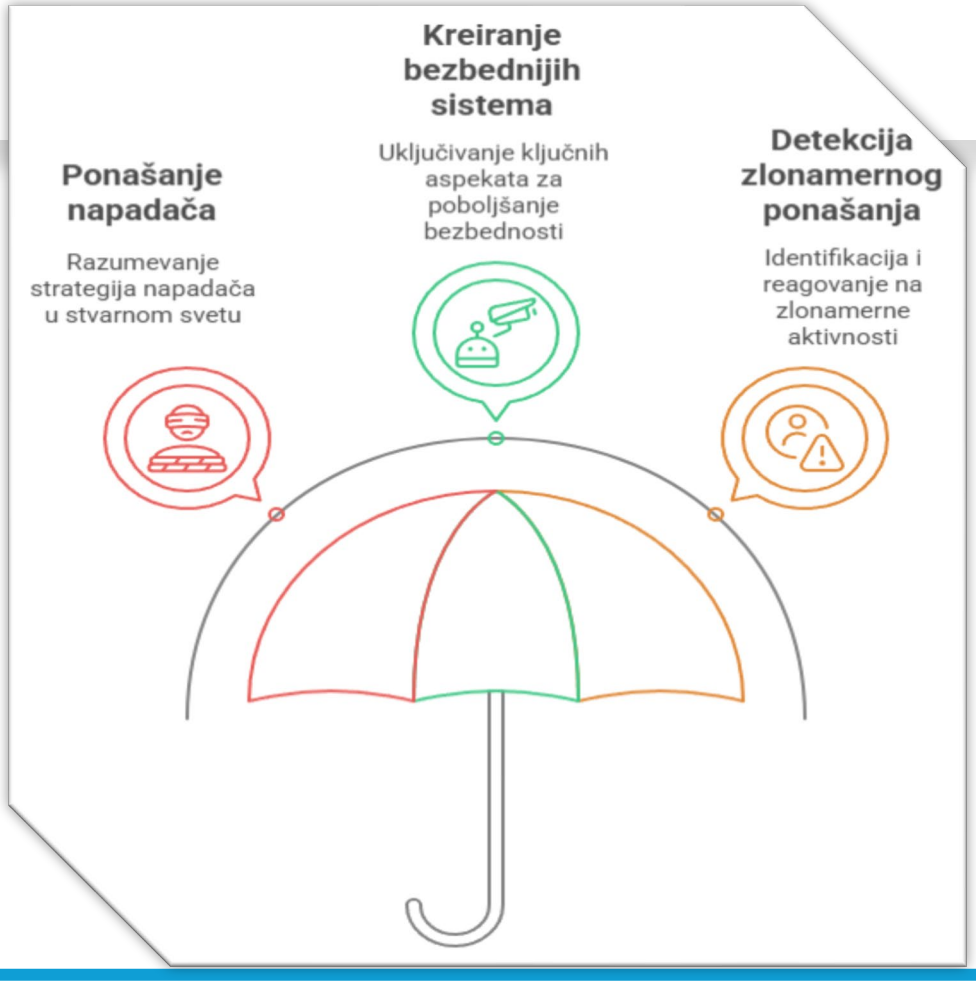
Predavač: dr Dušan Stefanović

Administratori Sistema
Zainteresovani za upravljanje i održavanje bezbednih sistemskih infrastruktura.

Programeri
Znanje o integraciji sigurnosnih mera tokom procesa razvoja softvera.

Security Analisti
Teže specijalizaciji u analizi i upravljanju rizicima od pretnji.

ŠTA ĆETE NAUČITI



KLJUČNE VEŠTINE

Računarske veštine

Razumevanje operativnih sistema i softverskih sistema za identifikaciju ranjivosti.

Mrežne veštine

Poznavanje mrežne infrastrukture i protokola za zaštitu mreža.

Životne veštine

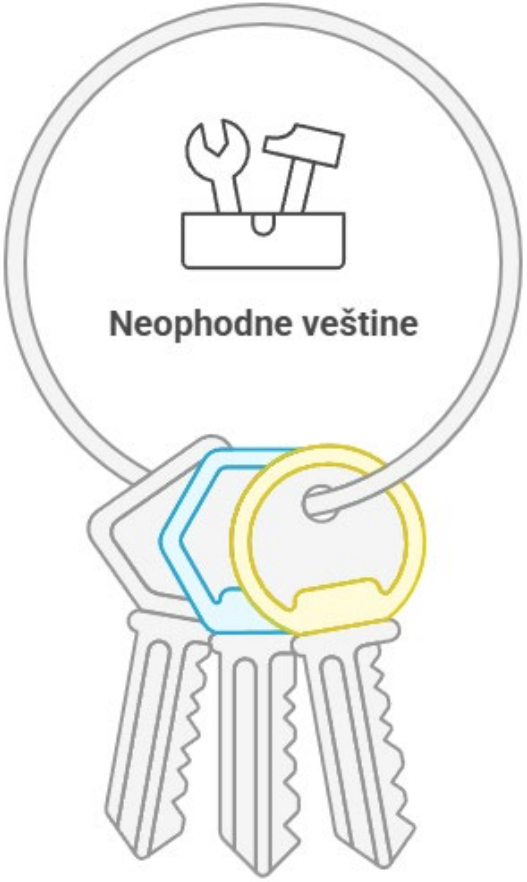
Kreativno razmišljanje i upornost za prevazilaženje izazova u sajber bezbednosti.

Kriptografija

Razumevanje enkripcije i zaštite podataka.

Digitalna forenzika

Istraživanje sajber napada i ranjivosti.



Alati

Veštine potrebne za efikasno korišćenje i upravljanje raznim alatima.

Mreže

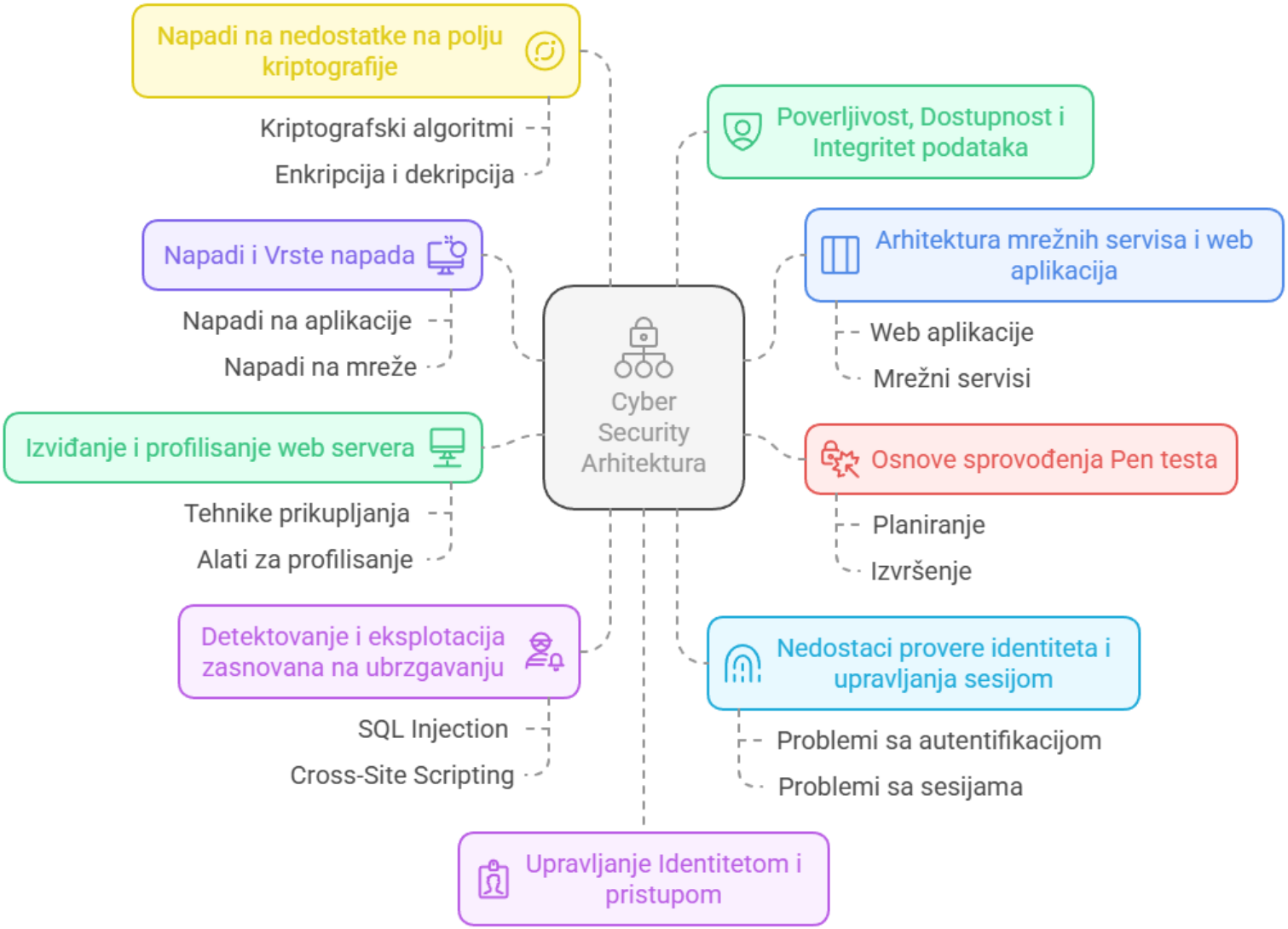
Duboko razumevanje mrežnih protokola i sigurnosnih mera.

Metode

Strategije za optimizaciju resursa i primenu prikupljenih saznanja.

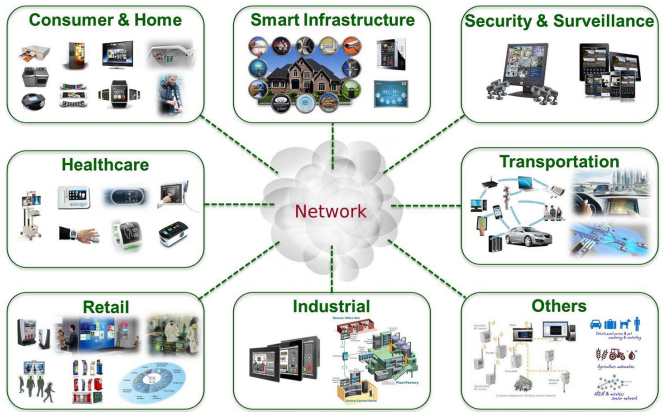
KLJUČNE VEŠTINE

SADRŽAJ PREDMETA



WEB APLIKACIJE

Tip aplikacije koji je danas najzastupljeniji u svim kompanijama



Aplikacije za mobilne telefone i IoT uređaji koriste web komponente kroz web servise i interfejse koji su ugrađeni u njih

POTREBA ZA BEZBEDNIM WEB APLIKACIJAMA

Web serveri i web aplikacije su atraktivne mete za napadače zbog velikog broja web sajtova na Internetu i organizacija koje svoje poslovanje obavljaju online.

Za interakciju sa web aplikacijom dovoljan je samo pretraživač (web browser)

POTREBA ZA BEZBEDNIM WEB APLIKACIJAMA

Sajber kriminalci ostvaruju znatne finansijske dobitke eksploatisanjem web aplikacija

Instaliranjem zlonamernih programa koji se prosleđuju korisnicima aplikacija

POTREBA ZA BEZBEDNIM WEB APLIKACIJAMA

HTTP saobraćaj je dozvoljen od strane firewall-a, napadačima nisu potrebni posebni otvoreni portovi.

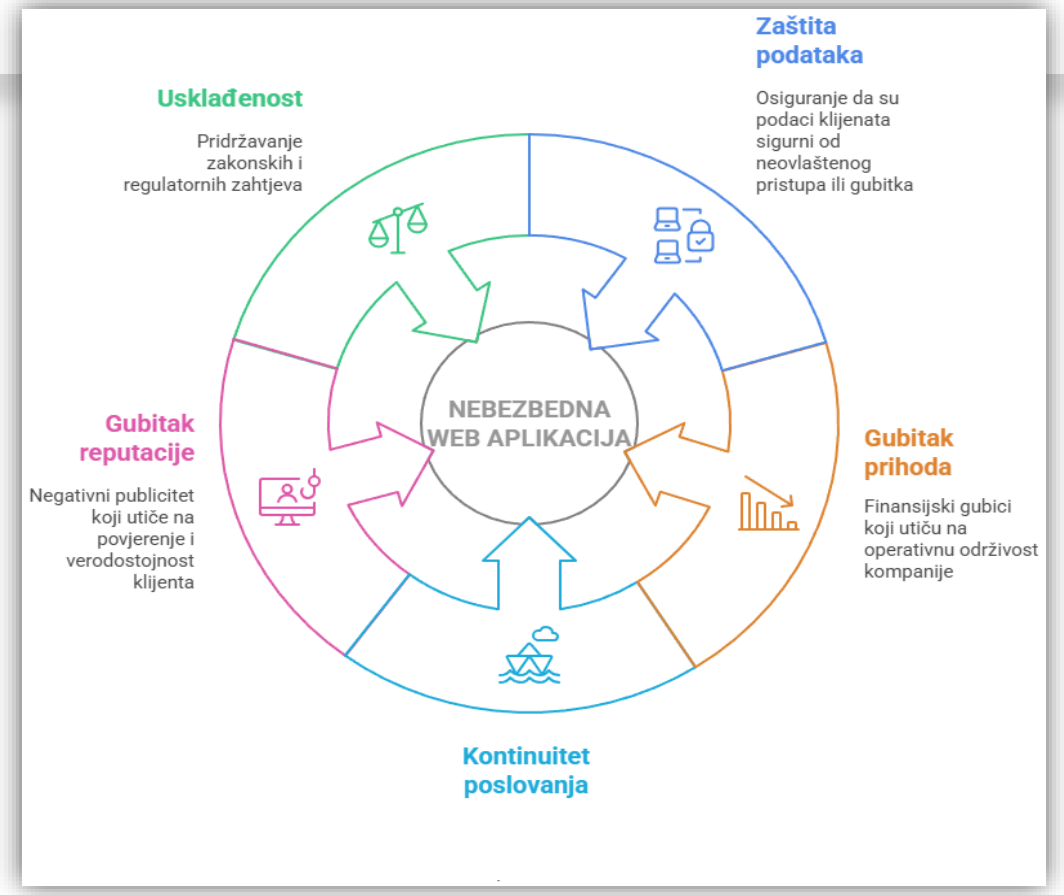
HTTP protokol nema ugrađene bezbednosne funkcije, ne obezbeđuje identifikaciju individualnih sesija što znači da je na programeru da ih dizajnira.

POTREBA ZA BEZBEDNIM WEB APLIKACIJAMA

Bezbednost se uključuje u fazi projektovanja aplikacije.

Kasnije integrisanje bezbednosti je veoma teško i zahteva prilično prerade koda.

POTREBA ZA ZAŠTITIOM OD NAPADA NA WEB APLIKACIJE



ZAŠTO JE TEŠKO ZAŠTITITI RAČUNARSKI SISTEM

Kod koji sadrži greške u smislu bezbedonosnih propusta i koji se ne pridržava preporuka koje se odnose na bezbednost

Socijalni inženjering – prevarom do poverljivih informacija

ZAŠTO JE TEŠKO ZAŠTITITI RAČUNARSKI SISTEM

- Novac može da se zaradi traženjem i eksplotacijom ranjivih aplikacija
- Market gde mogu da se nađu i kupe informacije o ranjivim aplikacijama
- Market za ukradene podatke koji su van kontrole vlasnika
- Postoji mnogo načina da se uzme profit od ukradenih podataka ili kompromitovanih mašina

SAJBER PRETNJE

	Nacionalni akteri	Sajberkriminalci	Haktivisti [hakeri aktivisti]
CILJ	Špijunaža, sabotaža, operacije uticaja	Finansijska korist kroz krađu, prevaru ili iznudu	Promocija političkih ili društvenih ciljeva
MOTIVI	Politička, ekonomska, vojna prednost	Finansijska dobit, oportunizam	Ideološki, publicitet
PRIMERI	APT28 (Fancy Bear), APT29 (Cozy Bear)	REvil, Conti ransomware grupe	Anonymous, LulzSec

SAJBER PRETNJE POKRENUTE VEŠTAČKOM INTELIGENCIJOM

Uspon veštačke inteligencije (AI) će omogućiti sajberkriminalcima da pokrenu sofisticiranije napade, kao što su phishing kampanje generisane AI-jem, društveni inženjering zasnovan na deepfake tehnologiji i autonomni malveri.

RIZICI KVANTNIH RAČUNARA

Predstavlja značajnu pretnju za trenutne standarde enkripcije.

Kvantni računari bi mogli da razbiju tradicionalne kriptografske algoritme, čineći mnoge bezbednosne sisteme zastarelim

RANJIVOST U IOT UREĐAJIMA

Eksponencijalni rast IoT uređaja i *edge computing* stvoriće veću površinu za napade.

Mnogi uređaji nemaju robusnu zaštitu, što ih čini lakim ciljevima za sajber napade.