SVEUČILIŠTE U ZAGREBU
Fakultet elektrotehnike i računarstva

Diplomski studij

Sigurnost komunikacija

Ak. godina 2021/2022

Osnovni pojmovi

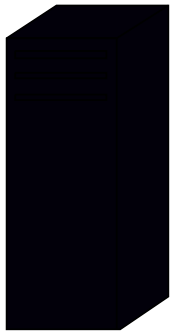
Creative Commons

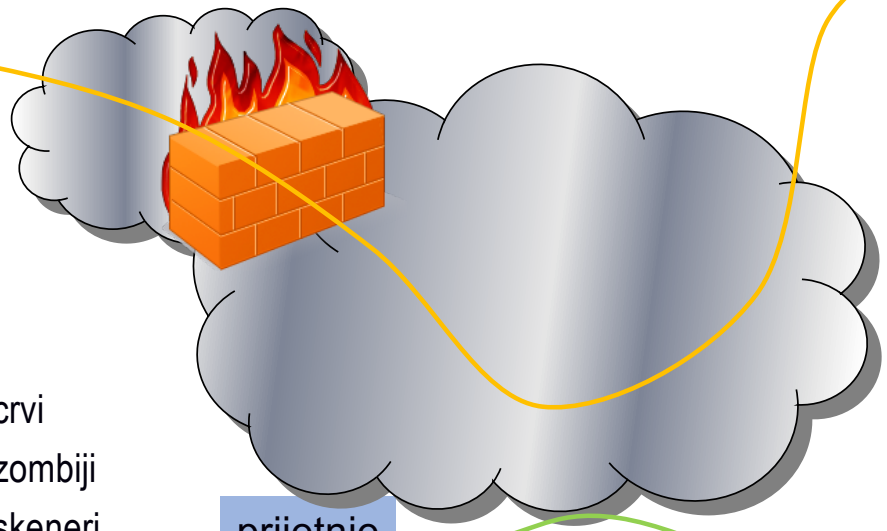
- **slobodno smijete:**
  - **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
  - **remiksirati** — prerađivati djelo
- **pod sljedećim uvjetima:**
  - **imenovanje**. Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
  - **nekomercijalno**. Ovo djelo ne smijete koristiti u komercijalne svrhe.
  - **dijeli pod istim uvjetima**. Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencom koja je ista ili slična ovoj.

U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu. Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Tekst licencije preuzet je s http://creativecommons.org/.

Sigurnost mreža, usluga i aplikacija





sigurnost mreže

sigurnost aplikacije

- virusi
- hoax
- malware
- spyware
- adware
- dialeri
- trojanci

- antivirus

- crvi
- zombiji
- skeneri

- firewall
- Intrusion Detection System

prijetnje rješenja

- IPsec
- demilitarizirana zona
- virtualne privatne mreže

sigurnost aplikacija i usluge

- cross site scripting
- ranjivosti
- Denial of Service
- lozinke
- lažna sjedišta

- kriptografija

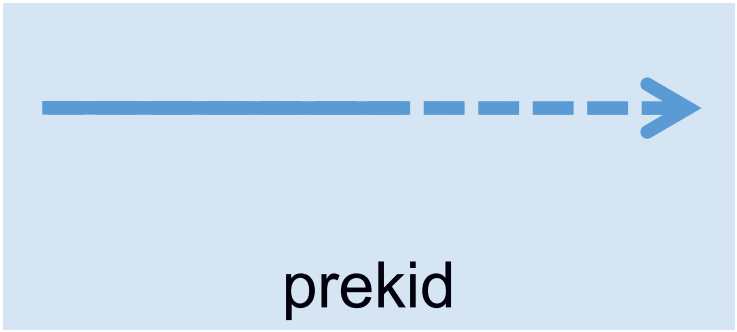
Ranjivost, prijetnja, napad, nadzor

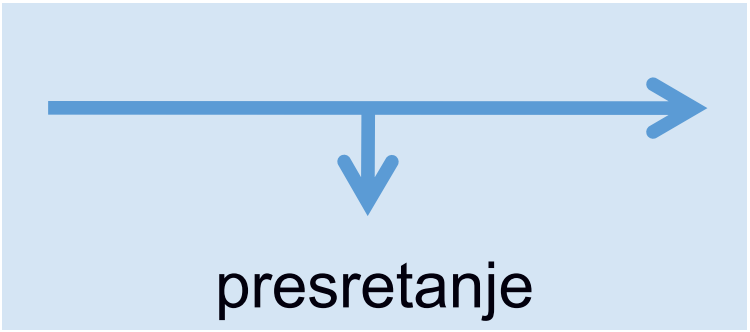
- mogući ciljevi: sklopovlje, programska podrška, podaci
- ranjivost:
  - slabost u izvedbi sustava koju je moguće iskoristiti kako bi se izazvala šteta
- prijetnja:
  - skup okolnosti koji može nanijeti štetu
- napad:
  - postupak u kojem se iskorištava ranjivost sustava
- nadzor:
  - mjere predostrožnosti
- prijetnja se sprječava nadzorom ranjivosti

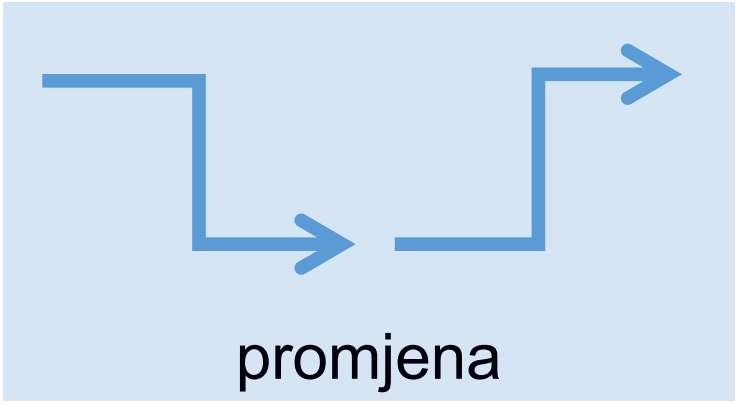
Pojam prijetnje

- prijetnja u mrežnom okruženju - okolnost, stanje ili događaj
  - cilj:
    - osoblje, mrežni ili računalni resursi
  - metode:
    - uništavanje, razotkrivanje ili modifikacija podataka
    - uskraćivanje usluge
    - prijevara
    - zlouporaba
  - vrste:
    - namjerna ili slučajna
    - aktivna ili pasivna
    - unutarnja ili vanjska

Metode

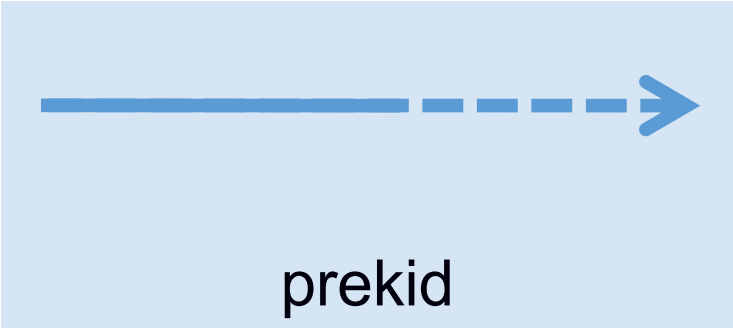






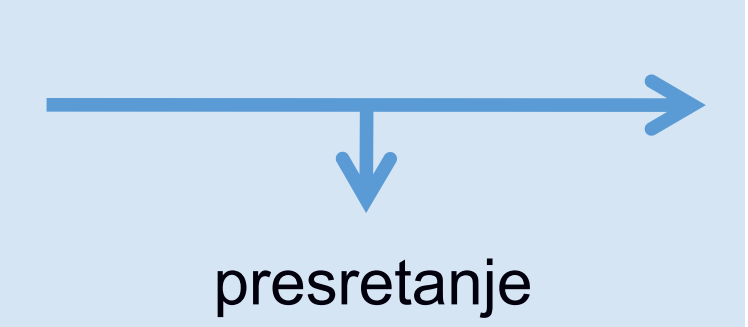
Prekidanje komunikacije

- sustav nestaje, biva nedostupan ili neiskoristiv
  - uništavanje sklopovlja
  - fizičko uništavanje komunikacijskih medija
  - ometanje komunikacije (šum)
  - narušavanje tablica usmjeravanja
  - brisanje programa ili datoteka
  - uskraćivanje usluge
  - Ukrajina 2022.!



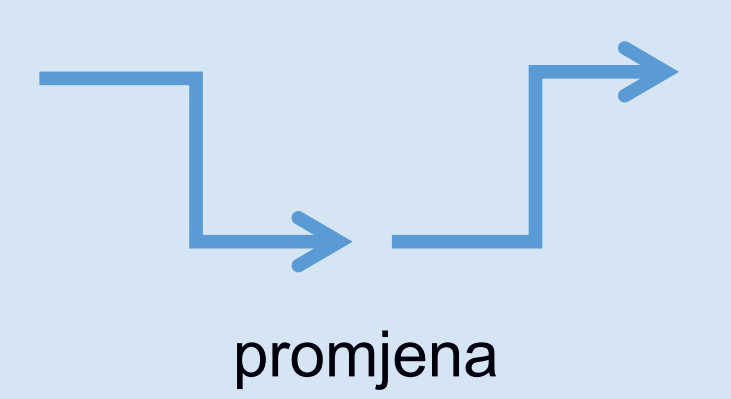
Presretanje

- neovlaštena osoba ima pristup sustavu
  - prisluškivanje (*eavesdropping*)
  - nadzor mrežne komunikacije (*link monitoring*)
  - snimanje mrežnog prometa (*packet capturing*)
  - kompromitacija sustava (*system compromisation*)
- teško izbjeći kod bežične komunikacije i višeodredišnog i grupnog razašiljanja



Promjena podataka

- neovlaštena osoba mijenja sustav
  - mijenjanje zapisa u bazi podataka
  - kompromitiranje sustava
  - zlonamjerno iskorištavanje zastoja u komunikaciji
  - promjena sklopovske podrške



Ubacivanje lažne informacije

- neovlaštena osoba stvara lažne informacije
  - dodavanje novih zapisa u bazu podataka
  - ubacivanje IP-datagrama u mrežu (*IP spoofing*)
  - lažne elektroničke poruke
  - lažna web-sjedišta

Metode, prilike i motivi

- zlonamjerni napadač zadovoljava 3 uvjeta:
  - metoda:
    - vještina, znanje, alati i ostalo što mu omogućuje da izvede napad
  - prilika:
    - vrijeme i pristup sustavu
  - motiv:
    - razlog zbog kojeg želi napasti sustav
- često su mete sustavi koji imaju mnogo korisnika
  - Windows, IE...

Napadi iznutra

- iz sustava i korisnika koji su pod nadležnošću administratora
- autorizirani korisnici - saboteri
  - većinom slučajne greške, šteta nije zanemariva!
- zloupotreba ovlasti kod administratora
- djelatnici koji imaju pristup sustavu ali nisu zaduženi za uslugu

Napadi izvana

- kriminalne ili terorističke organizacije
- obavještajne službe
- komercijalna poduzeća (industrijska špijunaža)
- istražiteljske agencije
- državne agencije
- hackeri i *script-kiddies*

Načini napada

- elektronički
  - neautorizirani pristup sustavu
    - problemi konfiguracije, pogrešne ovlasti za pristup
  - računalni virusi
  - privremeno uskraćivanje usluge
- ostale metode
  - krađa opreme, provale
  - prijevara: društveni inženjering
  - plansko postavljanje agenata unutar sustava
  - poricanje korištenja usluga i izbjegavanje obaveza
  - krivotvorenje dopuštenja za pristup sustavu
  - krađa lozinki ili kartica za pristup

Osnovni sigurnosni zahtjevi

- povjerljivost (*confidentiality*)
- cjelovitost, integritet (*integrity*)
- raspoloživost (*availability*)

} CIA

- autentifikacija (*authentification*)
- neporecivost (*nonrepudiation*)
- kontrola pristupa (*access control*)

- ranjivi:
  - sklopovlje
  - programska podrška
  - podaci

Cjelovitost

- cilj IS: zaštititi podatke od neovlaštenog brisanja, mijenjanja ili bilo kakve manipulacije bez prethodne autorizacije
- načela uspostave kontrole cjelovitosti su:
  - dodjela samo nužnih prava pristupa (engl. *need-to-know basis*)
    - ograničavanjem prava pristupa povećava se razina sigurnosti ali i složenost samog sustava
    - pronaći zadovoljavajuću razinu sigurnosti i praktične produktivnosti
  - odvajanje dužnosti (engl. *separation of duties*)
    - raspodjela odgovornosti nad ključnim dijelovima procesa na barem dvije fizičke osobe sa istim privilegijama
  - rotacija dužnosti (engl. *rotation of duties*)
    - rotacija zaposlenika na sličnu dužnost povećava internu razinu kontrole i smanjuje mogućnost napada

Povjerljivost

- cilj IS-a: identifikacija i autentifikacija korisnika
- najčešće prijetnje povjerljivosti :
  - hakiranje - preuzimanje kontrole iskorištavanjem sigurnosnih slabosti sustava
  - maskiranje - pristup resursima koristeći neovlašteno pribavljene tuđe autorizacijske podatke
  - nezaštićeno preuzimanje datoteka - prijenos datoteka u okruženje dostupno neovlaštenim korisnicima
  - trojanski konji
- napadi se odnose i na narušavanje svojstva cjelovitosti

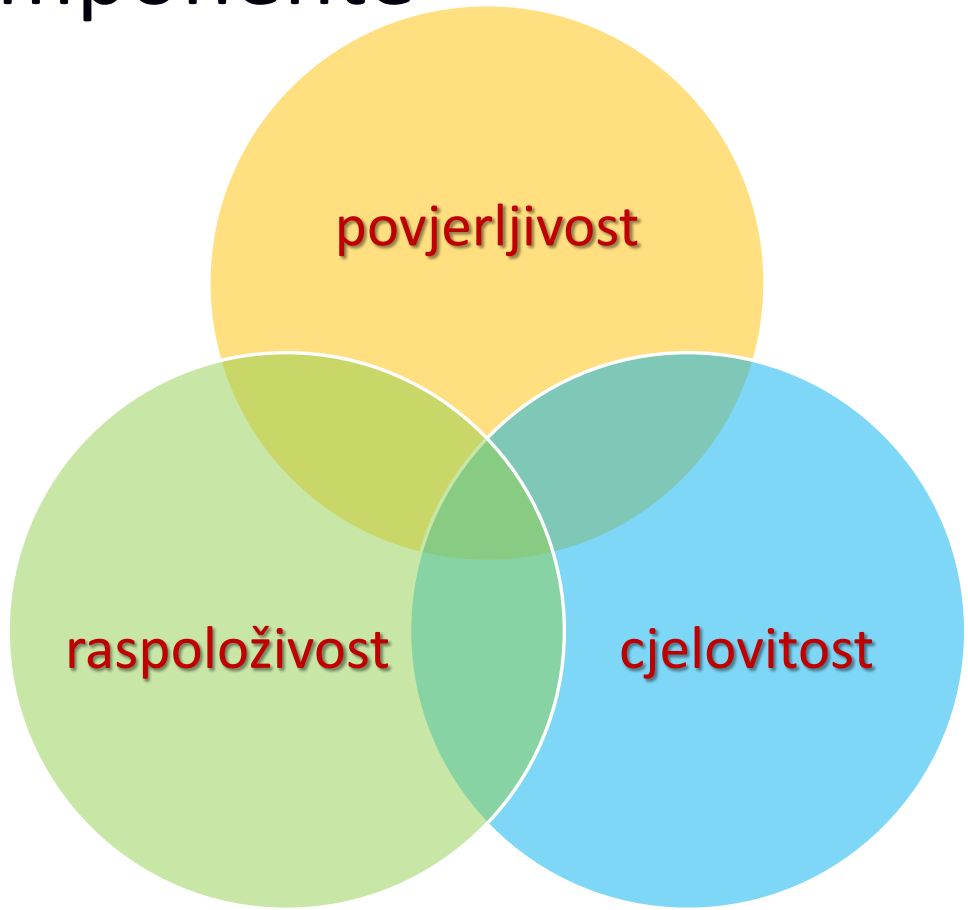
- još: tajnost, privatnost

Raspoloživost

- cilj IS-a: dostupnost tražene usluge u promatranom trenutku ili u definiranom vremenskom rasponu usprkos mogućim neočekivanim i nepredvidljivim događajima

- smanjenje ili uskraćivanje raspoloživosti radi:
  - napada uskraćivanjem usluge (engl. Denial of Service)
  - gubitak sposobnosti obrade podataka kao rezultat prirodnih katastrofa ili nedostatka temeljnih potreba sustava (struja, hlađenje)

Odnos 3 komponente



Autentifikacija

- autentifikacija:
  - potvrda autentičnosti korisnika
    - odgovarajuće metode primjenjuju se ovisno o aplikaciji i uslugama koje ih koriste
  - razlika: identifikacija – autentifikacija
- neporecivost:
  - sudionici ne mogu odbiti ili poreći akciju u kojoj su sudjelovali, npr. slanje i primanje informacija
- kontrola pristupa:
  - ograničavanje pristupa informacijama i ograničavanje provođenja akcija

Ranjivosti sustava

- *malware (malicious software)*
  - softver kojem je svrha infiltracija i oštećenje računala
    - *spyware* i *adware* (uglavnom napad na privatnost)
    - virusi
    - crvi
    - trojanci
    - *dialeri*
- lažne poruke *(hoax)*
  - poruke neistinitog sadržaja
- društveni inženjering
- društvene mreže
- mobilni uređaji

Pojam sigurnosti

- sigurnost mreža, usluga i aplikacija – bitna za stvaranje povjerenja
  - sposobnost informacijskog sustava da se odupre neočekivanim događajima i neprijateljskim akcijama
  - mogući ciljevi napada:
    - raspoloživost
    - vjerodostojnost
    - integritet
    - povjerljivost
- ranjivost je posljedica sigurnosne slabosti i nedostataka
  - napadač to iskorištava za kompromitaciju i neovlašten pristup
- rješenje: nadzor i kontrola ranjivosti

Osiguravanje mehanizama I

- definirati uloge, odgovornosti i nadležnosti za sve korisnike
- dokumentirati mrežnu arhitekturu
- identificirati kritične sustave ili sadrže osjetljive informacije koje zahtijevaju dodatne razine zaštite
- ostvariti rigorozni postupak upravljanja rizicima
- uspostaviti strategiju obrane mreže temeljenu na načelu dubinske obrane
- jasno definirati zahtjeve za sigurnost

Osiguravanje mehanizama II

- ustrojiti učinkovite postupke za konfiguraciju sustava
- provoditi rutinsko samoprocjenjivanje
- ustrojiti postupke za „backup“ sustav i spašavanje podataka u slučaju nesreće
- organizacija mora uspostaviti očekivanja vezana uz sigurnost i odrediti pojedince odgovorne za provođenje sigurnosti
- osigurati mehanizme koji će spriječiti vjerojatnost da članovi organizacije slučajno otkriju osjetljive informacije vezane uz mrežu

Primjer: sigurnost alata za video konferencije

COVID-19 i rast korisnika…

- ZOOM: 300 milijuna sudionika dnevno (travanj2020)
  - 10 milijuna u prosincu 2019.
- MSTeams: 75 milijuna sudionika dnevno (travanj 2020)
  - +70% od prosinca 2019.
- Ostali: npr. Webex oko 250.000 dnevno (travanj 2020)
- Dobar primjer:
  - kako sigurnost često nije u prvom (a ni u drugom?) planu
  - kako napadi rastu proporcionalno broju korisnika

Zoom i ranjivosti (3/4/5 2020.)

- Zoom i Facebook SDK
  - Razmjena zbog funkcionalnosti „prijava putem Facebooka”
  - Nova verzija više ne podržava razmjenu podataka s Facebookom

- Zoom bombing
  - infiltracija napadača u videokonferencije drugih korisnika, uz neprimjerene poruke, prijetnje i ucjene
  - pozivi za videokonferencije bili javno dostupni, bez kontrole pristupa – naknadno uvedene „čekaonice”, lozinke, mogućnost prijave napadača (eng. Report a user)
  - kompleksniji meetingID – teže za nasumično pogađanje

Zoom i ranjivosti (3/4/5 2020.)

- Zoom @Windows ranjivosti
  - krađa korisničkih podataka – hash lozinke – putem UNC-a
  - 0-day: *remote code execution* – kroz datoteke, bez upozorenja korisniku

- Šifriranje s kraja na kraj? - tek u srpnju 2020!
  - do tada moguće: lažne poruke, povjerljivost…
  - Problem: spajanje putem drugih mreža (npr. PSTN)

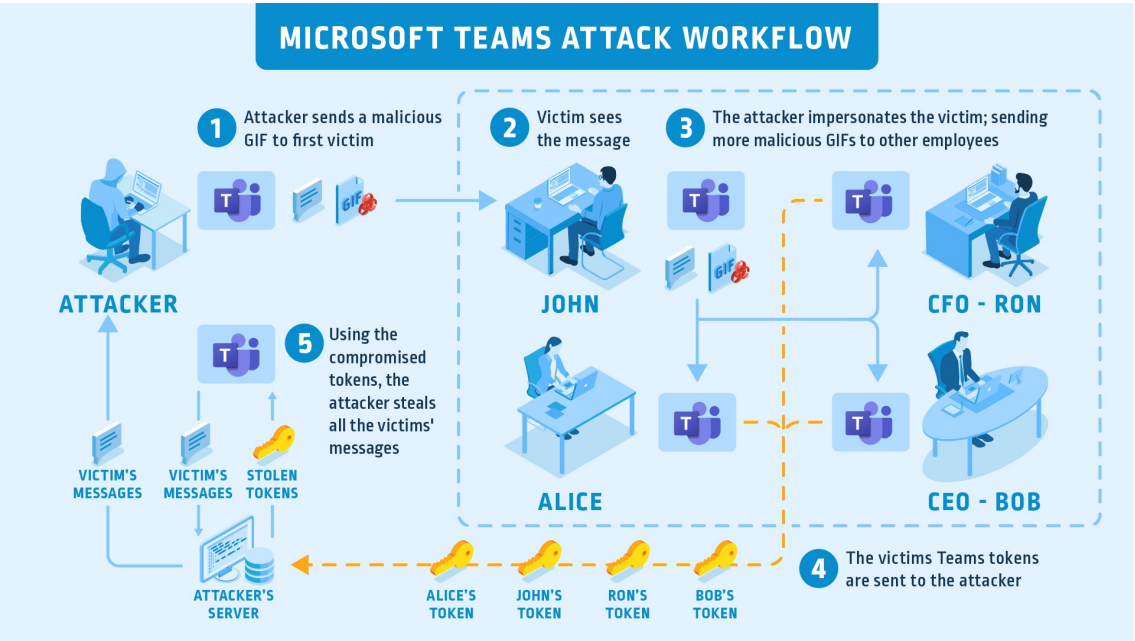
- Company Directory
  - automatsko dodavanje korisnika na listu kontakata ukoliko su pripadnici iste poslovne organizacije
  - pogrešne postavke Zooma - otkrivanje podataka drugih korisnika na istoj domeni (e-mail, profili, slanje zahtjeva)

Zoom i ranjivosti (3/4/5 2020.)

- Zoom i LinkedIn Sales Navigator
  - povezivanje korisnika Zooma i korisnika LinkedIna i prikupljanje podataka u svrhu marketinga
- zWarDial
  - alat za automatiziranu pretragu meeting ID oznaka, nekada moguće pristupiti bez lozinke
- Snimke video poziva
  - Jednostavan algoritam imenovanja snimki pohranjenih u nezaštićenom ”oblaku”
- 500,000 Zoom korisničkih računa na dark webu!

MS Teams i ranjivosti (3. 2020.)

- ”GIF ranjivost”
  - Problem s *tokenima*



https://www.cyberark.com/resources/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams

Zakonska regulativa

(Republika Hrvatska i EU)

KAZNENA DJELA PROTIV RAČUNALNIH SUSTAVA, PROGRAMA I PODATAKA

- Kazneni zakon (NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21)
- Glava XXV. Članci 266 – 273
  - **Neovlašteni pristup**
  - Ometanje rada računalnog sustava
  - Oštećenje računalnih podataka
  - Neovlašteno presretanje računalnih programa
  - Računalno krivotvorenje
  - Računalna prijevara
  - Zloupotreba naprava
  - Teška kaznena djela protiv računalnih sustava, programa i podataka

Kibernetička sigurnost

- EU Regulativa
  - Direktiva 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194) – Poznata pod nazivom „NIS Direktiva“
  - Svrha: Osigurati da zemlje EU-a budu pripravne i spremne na rješavanje kibernetičkih napada
- HR zakonodavstvo
  - Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18)
  - Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 68/18)
  - Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za njezinu provedbu (NN 108/15)

Kritična infrastruktura

- EU Regulativa
  - Direktiva 2008/114/EZ o utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite (SL L 345)
  - Svrha: Identificirati europsku kritičnu infrastrukture i poboljšati njenu zaštitu od svih vrsta prijetnji i opasnosti
- HR zakonodavstvo
  - Zakon o kritičnim infrastrukturama (NN 56/13)

Elektroničko poslovanje

- EU Regulativa
  - Uredba(EU) 910/2014 o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu (SL L 257) – Poznata pod nazivom „eIDAS Uredba“
  - Svrha: Povećati povjerenje u online usluge i elektroničku trgovinu te osigurati uzajamno priznavanje elektroničke identifikacije među članicama EU
- HR zakonodavstvo
  - Zakon o provedbi Uredbe (EU) 910/2014 (NN 62/17)

Elektroničke komunikacije

- EU Regulativa
  - Direktiva (EU) 2018/1972 o Europskom zakoniku elektroničkih komunikacija (SL L 321)
  - Svrha: Reguliranje elektroničkih komunikacijskih mreža i usluga, povezane opreme i usluga, poboljšati suradnju na razini EU te potaknuti razvoj 5G i mreža velikog kapaciteta
- HR zakonodavstvo
  - Zakon o elektroničkim komunikacijama (NN 73/08, 90/11, 133/12, 80/13, 71/14, 72/17)

Pristupačnost

- EU regulativa
  - Direktiva (EU) 2016/2102 Europskog parlamenta i Vijeća od 26. listopada 2016. o pristupačnosti internetskih stranica i mobilnih aplikacija tijela javnog sektora (SL L 327)
  - Svrha: Poboljšati pristupačnost internetskih stranica i mobilnih aplikacija tijela javnog sektora i omogućiti lakši pristup javnim uslugama, posebice osobama s invaliditetom.
- HR zakonodavstvo
  - Zakon o pristupačnosti mrežnih stranica i programskih rješenja za pokretne uređaje tijela javnog sektora (NN 17/2019)

Zaštita osobnih podataka

- EU regulativa
  - Uredba (EU) 2016/679 o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (SL L 119)
  - Svrha: Građanima omogućiti bolju kontrolu nad njihovim osobnim podatcima, a poduzećima olakšati korištenje i prenošenje osobnih podataka
- HR zakonodavstvo
  - Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18)

Pravo na pristup informacijama

- EU regulativa
  - Direktiva (EU) 2019/1024 o otvorenim podatcima i ponovnoj uporabi informacija javnog sektora (SL L 172)
  - Svrha: Olakšati pristup i korištenje informacija javnog sektora i državne uprave, ojačati podatkovno gospodarstvo EU i pospješiti razvoj umjetne inteligencije
- HR zakonodavstvo
  - Zakon o pravu na pristup informacijama (NN 25/13, 85/15)

Zaštita klasificiranih podataka

- EU regulativa
  - Odluke Vijeća 2013/488/EU i 2015/444 o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a i njena (SL L 274, SL L 72)
  - Svrha: Zaštititi klasificirane podatke od neovlaštenog pristupa i otkrivanja
- HR zakonodavstvo
  - Zakon o tajnosti podataka(NN 79/07, 86/12)

Zaštita poslovne tajne

- EU regulativa
  - Direktiva (EU) 2016/943 o zaštiti neotkrivenih znanja i iskustva te poslovnih informacija (poslovne tajne) od nezakonitog pribavljanja, korištenja i otkrivanja (SL L 157)
  - Svrha: Zaštita od nezakonitog pribavljanja, korištenja i otkrivanja poslovnih tajni
- HR zakonodavstvo
  - Zakon o zaštiti neobjavljenih informacija s tržišnom vrijednosti (NN 30/18)

Zaštita autorskog prava i intelektualnog vlasništva

- EU regulativa
  - Direktiva 2001/29/EZ o usklađivanju određenih aspekata autorskog i srodnih prava u informacijskom društvu (SL L 167)
  - Direktiva 96/9/EZ o pravnoj zaštiti baza podataka (SL L 77)
  - Direktiva 2009/24/EZ o pravnoj zaštiti računalnih programa ((SL L 111)
  - Direktiva 2004/48/EZ o provedbi prava intelektualnog vlasništva (SL L 157)
  - Direktiva 2006/123/EZ o uslugama na unutarnjem tržištu (SL L 376)
  - Direktiva (EU) 2015/2436 Europskog parlamenta i Vijeća od 16. prosinca 2015. o usklađivanju zakonodavstava država članica o žigovima (SL L 336)
  - Svrha: Omogućujući zaštite autorskog prava intelektualnog vlasništva i potaknuti na suradnju među članicama EU
- HR zakonodavstvo
  - Zakon o autorskom pravu i srodnim pravima (NN 111/21)
  - Zakon o patentu (NN 16/20)
  - Zakon o žigu (NN 14/19)
  - Zakon o industrijskom dizajnu (NN 173/03, 54/05, 76/07, 30/09, 49/11, 46/18)
  - Zakon o naknadama u području intelektualnog vlasništva (NN 66/21)
  - Zakona o zastupanju u području prava industrijskog vlasništva (NN 54/05, 49/11, 54/13)