Univerzitetna založba
Univerze v Mariboru

Mihael Plevnik

Borut Jereb

UPRAVLJANJE INFORMATIKE IN INFORMACIJSKE

gradivo za vaje



Univerza v Mariboru
Fakulteta za logistiko

Upravljanje informatike in informacijske varnosti

Gradivo za vaje

Avtorja
Mihael Plevnik
Borut Jereb

November 2026

Naslov *Title*
Upravljanje informatike in informacijske varnosti
Managing Informatics and Information Security

Podnaslov *Subtitle*
Gradivo za vaje
Exercise Materials

Avtorja *Authors*
Mihael Plevnik
(Univerza v Mariboru, Fakulteta za logistiko; Slovenska vojska)

Borut Jereb
(Univerza v Mariboru, Fakulteta za logistiko)

Recenzija *Review*
Matevž Obrecht
(Univerza v Mariboru, Fakulteta za logistiko)

Rok Rupnik
(Univerza v Ljubljani, Fakulteta za računalništvo in informatiko)

Lektoriranje *Language editing*
Sonja Mlaker Kač
(Univerza v Mariboru, Fakulteta za logistiko)

Tehnična urednika *Technical editors*
Jan Perša
(Univerza v Mariboru, Univerzitetna založba)

Marina Bajić
(Univerza v Mariboru, Univerzitetna založba)

Oblikovanje ovitka *Cover designer*
Jan Perša
(Univerza v Mariboru, Univerzitetna založba)

Grafika na ovitku *Cover graphics*
Omrežje, avtor: geralt, pixabay.com, 2017

Grafične priloge *Graphic material*
Vsi viri so lastni, če ni navedeno drugače.
Vir ločni strani vseh ločnih poglavij je lasten, pripravljeno s pomočjo orodja UI.
Plevnik, Jereb (avtorja), 2026

Založnik *Published by*
Univerza v Mariboru
Univerzitetna založba
Slomškov trg 15, 2000 Maribor, Slovenija
https://press.um.si, zalozba@um.si

Izdajatelj *Issued by*
Univerza v Mariboru
Fakulteta za logistiko
Mariborska cesta 7, 3000 Celje, Slovenija
https://fl.um.si, info.fl@um.si

Izdaja *Edition*
Prva elektronska izdaja

Vrsta publikacije *Publication type*
E-knjiga

Izdano *Published at*
Maribor, Slovenija, november 2026

Dostopno na *Available at*
https://press.um.si/index.php/ump/catalog/book/1177

Izdano *Published at*
Maribor, Slovenija, november 2026

© Univerza v Mariboru, Univerzitetna založba
/ University of Maribor, University of Maribor Press

Besedilo / Text © Plevnik, Jereb (avtorja), 2026

To delo je objavljeno pod licenco Creative Commons Priznanje avtorstva-Nekomercialno-Brez predelav 4.0 Mednarodna. / *This work is licensed under the Creative Commons AttributionNonCommercialNoDerivs 4.0 International License.*

Uporabnikom je dovoljeno reproduciranje brez predelave avtorskega dela, distribuiranje, dajanje v najem in priobčitev javnosti samega izvirnega avtorskega dela, in sicer pod pogojem, da navedejo avtorja in da ne gre za komercialno uporabo.

Vsa gradiva tretjih oseb v tej knjigi so objavljena pod licenco Creative Commons, razen če to ni navedeno drugače. Če želite ponovno uporabiti gradivo tretjih oseb, ki ni zajeto v licenci Creative Commons, boste morali pridobiti dovoljenje neposredno od imetnika avtorskih pravic.

https://creativecommons.org/licenses/by-nc-nd/4.0/

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani
COBISS.SI-ID 304855555
ISBN 978-961-299-219-4 (PDF)

ISBN 978-961-299-219-4 (pdf)

DOI https://doi.org/10.18690/um.fl.8.2026

Cena *Price* Brezplačni izvod

Odgovorna oseba založnika *For publisher* Prof. dr. Dean Korošak, rektor Univerze v Mariboru

Citiranje *Attribution* Plevnik, M., Jereb, B. (2026). *Upravljanje informatike in informacijske varnosti: gradivo za vaje.* Univerza v Mariboru, Univerzitetna založba. doi: 10.18690/um.fl.8.2026

Univerzitetna založba
Univerze v Mariboru

Kazalo

1 Namen učbenika 1

2 Cilj učbenika 3

3 Struktura učbenika 5
1. sklop: Brskanje 5
2. sklop: HTML 5
3. sklop: Kibernetska varnost 6

4 Pomen učbenika za logistiko 7

1. Sklop: Brskanje 10
1 Uvod 11
2 Faze poteka komunikacije od URL do prikaza spletne strani 15
3 URL – naslov spletnega vira 21
3.1 Kaj je URL 21
3.2 Sestava URL 21
3.3 Protokoli v URL-jih 22
3.4 Kako brskalnik razume URL 22
3.5 Pomen za logistiko 22
3.6 Zakaj je to pomembno v praksi 23
3.7 Priporočila za logistična okolja 23
3.8 Varnostni vidiki 24
3.9 Primer 24
3.10 Vaja 1 – Prepoznaj dele URL-ja 25
3.11 Vaja 2 – Praktični preizkus 25
3.12 Povzetek 26
4 DNS – Domenski sistem imen 27
4.1 Kaj je DNS 27
4.2 Kako deluje DNS? 27
4.3 Osnovni zapisi v DNS 28
4.4 Primer poizvedbe 28
4.5 Pomen za logistiko 31
4.6 Zakaj je to pomembno v praksi 32
4.7 Priporočila za logistična okolja 33
4.8 Varnostni vidik 34
4.9 Tipične vaje / praktični koraki 34
4.10 Vaje 34
4.11 Povzetek postopka DNS preverjanja 35
5 Hosts datoteka 37
5.1 Povzetek 38
6 IPV4 naslovni prostor 39
6.1 Dolžina in zapis IPv4 naslovov 39
6.2 Zgodovinska razdelitev na razrede (A–E) 40
6.3 Tipične vaje / praktični koraki 41

6.4 Povzetek ... 43
7 Zasebni, javni in posebni naslovi (IPv4) ... 45
7.1 Javni naslovi ... 45
7.2 Zasebni naslovi (RFC 1918) ... 46
7.3 Tipične vaje / praktični koraki ... 47
7.4 Povzetek ... 51
8 ICMP ... 53
8.1 Kaj je ICMP? ... 53
8.2 Preverjanje ... 53
8.3 Preveri pot do cilja – tracert / traceroute ... 55
8.4 Dodatne možnosti ping ... 56
8.5 Preveri velikost paketov ... 56
8.6 Tipični rezultati in pomen ... 56
8.7 Pomen za logistiko ... 56
8.8 Zakaj je to pomembno v praksi? ... 58
8.9 Priporočila za logistična okolja ... 58
8.10 Varnostni vidik ... 58
8.11 Povzetek postopka preverjanja ICMP ... 59
8.12 Tipične vaje / praktični koraki ... 59
9 Port number – številke vrat ... 61
9.1 Kaj je port number? ... 61
9.2 Kako delujejo vrata? ... 61
9.3 Vrste vrat ... 62
9.4 Najpogosteje uporabljena vrata ... 62
9.5 TCP in UDP vrata ... 62
9.6 Pomen za logistiko ... 63
9.7 Zakaj je to pomembno v praksi? ... 64
9.8 Priporočila za logistična okolja ... 65
9.9 Varnostni vidiki ... 65
9.10 Tipične vaje / praktični koraki ... 66
9.11 Povzetek ... 68
10 NAT – Network Address Translation ... 69
10.1 Kaj je NAT ... 69
10.2 Zakaj potrebujemo NAT ... 69
10.3 Kako NAT deluje ... 70
10.4 Vrste NAT ... 70
10.5 PAT ... 70
10.6 Prednosti NAT ... 71
10.7 Slabosti NAT ... 71
10.8 Preveri NAT v praksi ... 72
10.9 Pomen za logistiko — NAT ... 72
10.10 Zakaj je to pomembno v praksi ... 73
10.11 Priporočila za logistična okolja ... 73
10.12 Varnostni vidik ... 74
10.13 Tipične vaje / praktični koraki ... 74
10.14 Povzetek postopka preverjanja NAT ... 76
11 ARP ... 77
11.1 Kaj je ARP ... 77
11.2 Zakaj potrebujemo ARP ... 77
11.3 Kako deluje ARP ... 78
11.4 Preverjanje ARP ... 78
11.5 Pomen za logistiko ... 80
11.6 Zakaj je to pomembno v praksi ... 82
11.7 Priporočila za logistična okolja ... 82
11.8 Varnostni vidik ... 83
11.9 Tipične vaje / praktični koraki ... 83
11.10 Vaje ... 84
11.11 Povzetek ... 84

12 MAC naslov ... 85
12.1 Kaj je MAC naslov ... 85
12.2 Zgradba MAC naslova ... 85
12.3 Vrste MAC naslovov ... 86
12.4 Kako MAC sodeluje pri prenosu podatkov ... 86
12.5 Prikaz MAC naslova v sistemu ... 86
12.6 MAC naslov in varnost ... 87
12.7 Pomen za logistiko ... 87
12.8 Zakaj je to pomembno v praksi ... 88
12.9 Priporočila za logistična okolja ... 89
12.10 Varnostni vidiki ... 89
12.11 Tipične vaje / praktični koraki ... 90
12.12 Povzetek ... 92
13 Ovijanje – pot podatkov skozi sloje omrežja ... 93
13.1 Kaj je enkapsulacija ... 93
13.2 Zakaj je enkapsulacija pomembna ... 93
13.3 OSI model in enkapsulacija ... 94
13.4 Kako poteka enkapsulacija ... 94
13.5 Primer: obisk spletne strani ... 95
13.6 Povzetek ... 96
14 Celoten potek – Od URL do prikaza spletne strani ... 97
14.1 Uvod ... 97
14.2 Potek komunikacije – korak za korakom ... 97
14.3 Povezava s konceptom varnosti ... 98
14.4 Shema poteka ... 98
14.5 Povzetek ... 100
15 Orodja ... 101
15.1 Notepad ++ (https://notepad-plus-plus.org/) ... 102
15.2 Sublime Text (https://www.sublimetext.com/) ... 103
15.3 Wireshark (https://www.wireshark.org/) ... 104
16 Sklep ... 107
Viri ... 109

2. Sklop: HTML ... 110
1 Uvod ... 111
2 Kaj je HTML ... 113
2.1 Kako je HTML nastal ... 113
2.2 Zakaj uporabljamo HTML? ... 114
2.3 Kaj pomeni izraz "obogateno besedilo"? ... 114
2.4 Kako deluje brskalnik? ... 115
2.5 Kako se HTML vključi v kontekst informatike in varnosti? ... 115
2.6 Datoteka HTML ... 115
2.7 Prvi koraki v praksi ... 116
2.8 Uporaba različnih orodij ... 116
2.8.1 Notepad: Vaš prvi HTML urejevalnik ... 117
2.8.2 Notepad++: Zmogljivejši urejevalnik kode ... 118
2.8.3 *Sublime Text*: Zmogljiv in prilagodljiv urejevalnik kode ... 120
3 Osnovna zgradba HTML dokumenta ... 123
3.1 Osnovna ideja ... 123
3.2 Vloga posameznih delov ... 124
3.2.1 Deklaracija ... 124
3.2.2 Koren ... 124
3.2.3 Glava dokumenta ... 124
3.3 Najpogostejši elementi v glavi dokumenta ... 125
3.4 Telo dokumenta ... 125
3.5 Kako brskalnik razume HTML ... 126
3.6 Primer za vajo v Notepadu ... 126
3.7 Povzetek ... 127

3.8 Naloga za samostojno delo ... 127
3.9 Vaje za poglavje 2 – Kaj je HTML ... 127
4 Osnovne HTML oznake za besedilo – naslovi, odstavki, povezave in slike ... 131
4.1 Uvod ... 131
4.2 Naslovi ... 131
4.3 Odstavki ... 132
4.4 Povezave ... 133
4.5 Slike ... 134
4.6 Absolutne in relativne poti pri povezavah ... 134
4.6.1 Absolutne poti ... 134
4.6.2 Relativna pot ... 135
4.6.3 Simboli pri relativnih poteh ... 136
4.6.4 Pogoste napake pri uporabi poti ... 136
4.7 Praktičen primer ... 137
4.8 Samostojna naloga ... 138
4.9 Povzetek ... 138
4.10 Vaje za poglavje 4 – Osnovne HTML oznake za besedilo: naslovi, odstavki, povezave in slike ... 138
5 Struktura spletne strani – uporaba seznamov, tabel in razdelkov (header, nav, main, footer). 147
5.1 Uvod ... 147
5.2 Kaj pomeni semantična struktura? ... 147
5.3 Osnovna postavitev strani ... 148
5.4 Uporaba seznamov ... 149
5.4.1 Neurejen seznam (oznaka s pikami) ... 149
5.4.2 Urejen seznam (številke) ... 150
5.5 Tabele ... 150
5.6 Naloga za samostojno delo ... 152
5.7 Povzetek ... 152
5.8 Vaje za poglavje 5 – Struktura spletne strani: seznami, tabele in razdelki ... 152
6 Osnove obrazcev (forms) – vnos podatkov, oznake in osnovna validacija ... 157
6.1 Kaj je obrazec v HTML? ... 157
6.2 Osnovna struktura obrazca ... 157
6.3 Najpogostejša polja za vnos ... 158
6.4 Oznake ... 158
6.5 Atributi za osnovno validacijo ... 159
6.6 Primer preprostega obrazca ... 159
6.7 Primer: dodajanje dodatnih polj ... 160
6.8 Kaj se zgodi, ko obrazec oddamo ... 161
6.9 Naloga za samostojno delo ... 161
6.10 Vaje za poglavje 6 – Osnove obrazcev (forms) ... 161
7 Razvoj HTML ... 165
8 Sklep ... 171
Viri ... 173

3. Sklop: Kibernetska varnost ... 174
1 Uvod ... 175
2 Teoretično razumevanje kibernetskega področja ... 177
2.1 Kibernetski prostor ... 178
2.2 Razmerja med pojmi varovanja kibernetskega prostora ... 182
2.2.1 Zagotavljanje informacijske varnosti ... 185
2.2.2 Informacijska varnost ... 187
2.2.3 Kibernetska varnost ... 189
2.2.4 Kibernetska obramba ... 190
2.2.5 Pojmovna zmeda ... 192
2.2.6 Razmerja med pojmi ... 193
2.3 Informacijsko-kibernetske grožnje ... 194
2.3.1 Opredelitev pojma kibernetske grožnje ... 195
2.3.2 Model kibernetskih groženj ... 196
2.3.3 Kibernetske grožnje ... 200

2.3.4 Primerjava kibernetskih groženj ... 203
3 Kibernetska varnost v NATU, EU in Sloveniji ... 207
3.1 Kibernetska varnost v NATU ... 207
3.1.1 Razvoj skozi deklaracije vrhov in kibernetska zaveza ... 207
3.1.2 Ukrepi za dvig kibernetske varnosti in operacije v kibernetskem prostoru ... 209
3.1.3 Pregled ugotovitev razvoja kibernetske varnosti NATA ... 210
3.2 Kibernetska varnost v EU ... 210
3.2.1 Strategija in zakonodaja ... 210
3.2.2 Investicije, znanja in ozaveščenost ... 211
3.2.3 Druga področja in pregled ugotovitev ... 211
3.3 Študija primera kibernetske varnosti Slovenije ... 212
4 Vaje ... 219
5 Rešitve ... 241
5.1 Vaja 1 ... 241
5.2 Vaja 2 ... 241
5.3 Vaja 3 ... 242
5.4 Vaja 4 ... 242
5.5 Vaja 5 ... 242
5.6 Vaja 6 ... 243
5.7 Vaja 7 ... 244
5.8 Vaja 8 ... 244
5.9 Vaja 9 ... 244
5.10 Vaja 10 ... 245
6 Sklep ... 247
Viri ... 249

1. SKLOP
BRSKANJE

Od vpisa spletnega naslova
do prikaza spletne strani



POT INFORMACIJE – KORAK ZA KORAKOM

1 URL – SPLETNI NASLOV

Uporabnik v brskalnik vpiše
spletni naslov, npr. https://www.example.com.
Brskalnik preveri, ali je naslov pravilen.

https://www.example.com

2 DNS – PREVOD IMENA V IP NASLOV

Brskalnik pošlje poizvedbo DNS strežniku,
ki prevede domeno (npr. www.example.com)
v IP naslov (npr. 93.184.216.34).
Rezultat se shrani v predpomnilnik.



3 TCP/IP – VZPOSTAVITEV POVEZAVE

Odjemalec vzpostavi povezavo do strežnika
na IP naslovu preko protokola TCP.
Uporabi se določen vrata
(npr. 443 za HTTPS).



4 NAT / ARP / MAC – LOKALNO OMREŽJE

Če smo v lokalnem omrežju, usmerjevalnik (NAT)
prevede zasebni IP naslov v javni.
ARP poišče MAC naslov naslednjega hopa
(npr. usmerjevalnika).



5 HTTP/HTTPS – PRENOS PODATKOV

Brskalnik pošlje zahtevo HTTP/HTTPS (npr. GET /).
Strežnik odgovori z vsebino (HTML, slike ...).
Podatki potujejo skozi omrežje v paketih.



6 PRIKAZ STRANI

Brskalnik prejete podatke razčleni,
izvede HTML, CSS in JavaScript,
ter prikaže spletno stran uporabniku.



DIAGNOSTIČNA ORODJA

ping · nslookup · netstat · Wireshark

VARNOST NA VSAKEM KORAKU

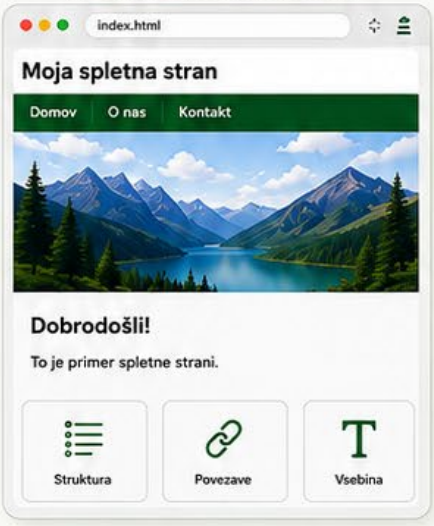
- Preverjaj URL – Preveri pravilnost spletnega naslova.
- Preveri digitalna – med odjemalcem in strežnikom.
- Bodi pozoren na omrežje – Razumevanje delovanja interneta je prvi korak do varne uporabe.

2. SKLOP
HTML

Od kode do spletne strani:
struktura, oznake in vsebina

```html
<!DOCTYPE html>
<html lang="sl">
<head>
  <meta charset="UTF-8">
  <title>Moja spletna stran</title>
</head>
<body>
  <header>
    <h1>Dobrodošli!</h1>
  </header>
  <nav>
    <a href="index.html">Domov</a>
    <a href="o-nas.html">O nas</a>
    <a href="kontakt.html">Kontakt</a>
  </nav>
  <main>
    <h2>Moja spletna stran</h2>
    <p>To je primer spletne strani,
      izdelane s HTML.</p>
  </main>
  <footer>
    <p>© 2026 Moja stran</p>
  </footer>
</body>
</html>
```

TO JE PRIMER SPLETNE STRANI.



OSNOVNI HTML ELEMENTI

- **STRUKTURA** – Osnova HTML dokumenta: <html>, <head>, <body>
- **VSEBINA** – Naslovi, odstavki, seznami, tabele, slike, povezave ...
- **POVEZAVE** – Ustvarimo povezave spletne strani
- **OBRAZCI** – Vnos podatkov in interakcija z uporabnikom
- **SEMANTIKA** – Uporaba semantičnih elementov za dostopnost in berljivost

POSTOPEK IZDELAVE SPLETNE STRANI.

1	2	3	4	5
NAČRTUJ	USTVARI	PREVERI	OBJAVI	OBJAVI
Strukturiraj vsebino.	Pišem HTML kodo.	Validacija s W3C orodjem.	Spletna stran je pripravljena.	Dodaš stil (CSS) in funkcionalnost (JavaScript).

Strukturirano. Semantično. Berljivo.
Dostopno. Validno. Združljivo.

3. SKLOP
KIBERNETSKA VARNOST

Zaščitimo informacije.
Zavarujmo organizacije.



KIBERNETSKE GROŽNJE

- **PHISHING** – Prevarantska sporočila za pridobitev občutljivih podatkov (gesla, bančni podatki ...).
- **MALWARE** – Zlonamerna programska oprema, ki okuži ali poškoduje sisteme.
- **RANSOMWARE** – Zlonamerna programska oprema, ki zaklene podatke in zahteva odkupnino.
- **APT (NAPREDNE TRAJNE GROŽNJE)** – Ciljani napadi z dolgotrajnim delovanjem, običajno s podporo organiziranih skupin.
- **DDoS NAPADI** – Preobremenitev strežnikov z velikim številom zahtev.
- **IZGUBA PODATKOV** – Izguba, kraja ali nenamerna izbris podatkov zaradi napake, napada ali nesreče.

UKREPI KIBERNETSKE VARNOSTI

- **Tveganja** – Prepoznavanje in ocena tveganj.
- **Zaščitni ukrepi** – Tehnični, organizacijski in kadrovski ukrepi.
- **Odzivanje in obnova** – Načrt, zaznavanje, odziv in obnova po incidentu.
- **Izobraževanje** – Zavedanje in usposabljanje uporabnikov.
- **Nadzor in spremljanje** – Neprekinjeno spremljanje sistemov in omrežja.

UREDITVE KIBERNETSKE VARNOSTI

NATO
- Politike in strategije
- Skupni standardi
- Zavezniška sodelovanja

EVROPSKA UNIJA
- NIS2 direktiva
- ENISA smernice
- DORA uredba
- GDPR varstvo podatkov

REPUBLIKA SLOVENIJA
- Zakon o informacijski varnosti (ZInfV)
- SI-CERT
- NKS organizacija
- Varovanje kritične infrastrukture

KIBERNETSKA VARNOST = EKIPNO DELO

LJUDJE · PROCESI · TEHNOLOGIJA · ZAVEDANJE

VARNOST NI IZDELEK, TEMVEČ PROCES.
ODGOVORNOST VSAKEGA IZMED NAS.

Univerzitetna založba
Univerze v Mariboru

1 Namen učbenika

Namen tega učbenika je študentom na praktičen in razumljiv način predstaviti pot informacije v digitalnem okolju organizacij: od njenega prenosa po računalniških omrežjih, prek njenega zapisa in predstavitve na spletu, do njenega varovanja pred sodobnimi kibernetskimi grožnjami. Učbenik v ta namen povezuje tri vsebinsko zaokrožene sklope: delovanje omrežne komunikacije od vpisa spletnega naslova do prikaza strani, osnove jezika HTML kot temeljnega orodja za strukturiranje in predstavitev informacij na spletu ter področje kibernetske varnosti kot okvir za razumevanje groženj, tveganj in odzivov nanje na ravni organizacij, držav in mednarodnih povezav.

Učbenik združuje teoretično razlago in praktične vaje. Namenjen je predvsem podpori praktičnemu delu in utrjevanju znanja, medtem ko so številne teoretične osnove praviloma podrobneje obravnavane v okviru predavanj ali drugih oblik študija. Študent skozi preproste primere in realne scenarije najprej razišče, kaj se v resnici zgodi, ko v brskalnik vpišemo spletni naslov (URL), in kako pri tem sodelujejo tehnologije, kot so DNS, TCP/IP, NAT, ARP in MAC, ter kako te procese opazujemo z diagnostičnimi orodji (ping, nslookup, netstat, Wireshark). Nato spozna, kako je spletna vsebina, ki jo brskalnik prejme, zgrajena. Torej spozna strukturo HTML dokumenta, pomen semantičnega označevanja ter samostojno izdelavo in validacijo enostavne spletne strani. V tretjem sklopu spozna kibernetski prostor, tipične informacijsko-kibernetske grožnje ter ureditev kibernetske varnosti v NATU, EU in Sloveniji.

Pri vseh treh sklopih se učbenik ne osredotoča le na tehnični vidik, temveč predvsem na varnostne posledice: kako posamezna plast omrežja vpliva na zaupnost, celovitost in razpoložljivost informacij, kako odgovorno objavljamo vsebine na spletu ter zakaj je kibernetska varnost ključna za neprekinjeno delovanje organizacij in logističnih procesov. Učbenik tako služi kot didaktično gradivo za vaje pri predmetu Informatika in

informacijska varnost v organizacijah ter študenta postopno vodi od osnovnih pojmov do samostojne uporabe znanja pri praktičnem delu.

Univerzitetna založba
Univerze v Mariboru

2 Cilj učbenika

Cilj učbenika je razviti celovito razumevanje poti informacije v digitalnem okolju. To pomeni razumevanje poti od njenega prenosa po računalniških omrežjih, prek njene predstavitve s spletnimi tehnologijami, do njenega varovanja ter ob tem krepiti sposobnost praktične uporabe znanja in zavedanje o varnostnih tveganjih, ki spremljajo vsak korak dela z informacijami v organizacijah.

Študent po predelavi vsebine in izvedbi vaj:

- razume, kako poteka komunikacija med odjemalcem in strežnikom, ter zna razložiti vlogo posameznega omrežnega protokola (DNS, IP, TCP, ARP, NAT, MAC),
- zna uporabiti osnovna diagnostična orodja (ping, nslookup, netstat, Wireshark) in povezati teoretične koncepte (OSI in TCP/IP model) s praktičnimi primeri,
- zna prepoznati tipične ranljivosti posameznih slojev omrežja in predlagati ustrezne obrambe,
- razume pomen in razvoj jezika HTML ter pozna osnovno strukturo HTML dokumenta (razliko med <head> in <body>),
- uporablja osnovne oznake za strukturiranje vsebine (naslovi, odstavki, povezave, slike, seznami, tabele, obrazci) in razloži pomen semantičnih elementov za dostopnost in berljivost,
- samostojno izdela preprosto spletno stran z več povezanimi podstranmi ter jo preveri s spletnim validatorjem W3C,
- razume pojem kibernetskega prostora, razmerja med pojmi varovanja ter tipične informacijsko-kibernetske grožnje,
- pozna ureditev kibernetske varnosti v NATU, EU in Sloveniji ter njen pomen za zaščito organizacij in kritične infrastrukture,

- spoštuje načela informacijske varnosti pri objavi spletnih vsebin (neobjavljanje osebnih podatkov, sklicevanje na licencirane vire, varna uporaba povezav),
- razvije sposobnost analitičnega razmišljanja pri odpravljanju težav ter razume pomen varnosti in odgovorne uporabe tehnologije v organizacijah in logističnih procesih.

Univerzitetna založba
Univerze v Mariboru

3 Struktura učbenika

Učbenik je zasnovan modularno in je razdeljen na tri vsebinsko zaokrožene sklope, ki študenta korak za korakom vodijo od razumevanja omrežne komunikacije, prek izdelave spletnih vsebin, do celovitega pogleda na kibernetsko varnost. Vsako poglavje združuje kratko razlago pojmov, praktične primere, pregledne tabele in naloge za samostojno delo, ki spodbujajo eksperimentalno učenje.

1. sklop: Brskanje

Sklop študenta popelje po celotni poti od vpisa spletnega naslova do prikaza strani. Po uvodu in pregledu faz komunikacije se po korakih obravnavajo URL, DNS in datoteka hosts, IPv4 naslovni prostor ter javni in zasebni naslovi, nato pa protokoli in mehanizmi ICMP, številke vrat, NAT, ARP in MAC naslovi. Sklop zaokrožita poglavji o ovijanju podatkov (angl. *data encapsulation*) skozi omrežne sloje in celotnem poteku komunikacije ter pregled diagnostičnih orodij (ping, nslookup, netstat, Wireshark), s katerimi študent opisane procese opazuje v praksi.

2. sklop: HTML

Sklop v petih povezanih poglavjih vodi od osnov jezika HTML do samostojne izdelave preproste spletne strani. Uvod predstavi temeljne pojme in zgodovinsko ozadje jezika, sledijo poglavja o osnovni zgradbi HTML dokumenta (elementa <head> in <body>), osnovnih oznakah za besedilo (naslovi, odstavki, povezave, slike), strukturi spletne strani s seznami, tabelami in semantičnimi razdelki (header, nav, main, footer) ter osnovah obrazcev z vnosom podatkov in osnovno validacijo. Sklop se zaključi z izdelavo spletne strani s tremi povezanimi podstranmi (index.html, tabela.html, kontakt.html).

3. sklop: Kibernetska varnost

Sklop najprej postavi teoretični okvir: opredeli kibernetski prostor, razmerja med pojmi varovanja kibernetskega prostora ter tipične informacijsko-kibernetske grožnje. Nato obravnava ureditev kibernetske varnosti v NATU in EU ter jo zaokroži s študijo primera kibernetske varnosti Slovenije. Sklopu so dodane vaje z rešitvami in seznam literature.

Vsak sklop se konča s povzetkom, ki ponovi bistvene koncepte, in vajami, s katerimi študent teoretično znanje preveri v praksi. Učbenik tako povezuje omrežja, spletne tehnologije in informacijsko varnost v celovit učni pripomoček, uporaben pri vajah, laboratorijskih analizah in samostojnem učenju.

Univerzitetna založba
Univerze v Mariboru

4 Pomen učbenika za logistiko

Sodobna logistika je v svojem bistvu upravljanje dveh tokov: toka blaga in toka informacij, pri čemer fizični tok brez informacijskega praktično ne deluje več. Informacijski tok pa je danes digitaliziran. Vsaka pošiljka, ki potuje po oskrbovalni verigi, ima svojo digitalno senco: naročilo v sistemu ERP, skladiščne transakcije v WMS, transportne naloge v TMS, elektronsko izmenjavo dokumentov med partnerji ter spletne portale za sledenje pošiljk. Vse te informacije potujejo po istih omrežnih poteh, so predstavljene z istimi spletnimi tehnologijami in izpostavljene istim grožnjam, kot jih obravnava ta učbenik. Zato razumevanje teh temeljev za strokovnjaka s področja logistike ni zgolj splošna računalniška pismenost, temveč poznavanje hrbtenice lastne stroke.

Znanje prvega sklopa (brskanje in omrežna komunikacija) strokovnjaku s področja logistike omogoča, da razume, kje in zakaj se informacijski tok lahko ustavi. Ko skladiščni terminal izgubi povezavo s strežnikom, ko se portal prevoznika ne odziva ali ko EDI sporočilo ne prispe do partnerja, zna z osnovnimi diagnostičnimi orodji vsaj okvirno prepoznati, ali gre za težavo z DNS, povezljivostjo, požarnim zidom ali strežnikom, in se s tehnično službo pogovarjati z argumenti, ne le z opisom simptomov. Drugi sklop (HTML) mu daje razumevanje, kako so zgrajeni spletni portali, obrazci za naročila in samodejno ustvarjena sporočila, s katerimi se v logistiki srečuje vsak dan; kdor pozna strukturo spletne strani, zna presoditi, katere podatke je varno objaviti, in hitreje prepozna ponarejeno stran ali obrazec, ki krade poslovne podatke.

Tretji sklop (kibernetska varnost) pa opozarja na dejstvo, da so oskrbovalne verige med najpogostejšimi tarčami kibernetskih napadov, saj povezujejo veliko število partnerjev z različnimi ravnmi zaščite. Primeri iz prakse, kot je napad NotPetya leta 2017, ki je ladjarju Maersk za več dni ohromil terminale po vsem svetu in povzročil za več sto milijonov dolarjev škode, kažejo, da izpad informacijskega sistema pomeni izpad fizične logistike: zaprta skladišča, stoječe tovornjake in ladje, ki jih ni mogoče razložiti. Logistična

infrastruktura, kot so pristanišča, železnice in distribucijski centri, je hkrati del kritične infrastrukture države, zato njena kibernetska odpornost presega interes posameznega podjetja.

Učbenik tako bodočemu strokovnjaku s področja logistike ne daje znanja strokovnjaka s področja informatike, temveč nekaj drugega: sposobnost, da informacijski tok razume, ga zna osnovno preveriti in ga odgovorno varuje. V poklicu, kjer zamuda informacije pomeni zamudo blaga, izguba podatkov pa lahko zaustavi celotno oskrbovalno verigo, je to znanje neposredna konkurenčna prednost in del poklicne odgovornosti.

1. SKLOP
BRSKANJE

Od vpisa spletnega naslova do prikaza spletne strani

Ko v brskalnik vpišemo spletni naslov (URL), se v ozadju izvede zapleten niz korakov, v katerih sodelujejo različni protokoli in omrežne tehnologije. Razumevanje tega procesa nam pomaga razumeti delovanje interneta in prepoznati varnostna tveganja.



POT INFORMACIJE – KORAK ZA KORAKOM

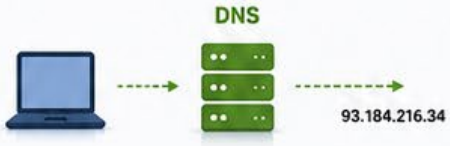
1 URL – SPLETNI NASLOV

Uporabnik v brskalnik vpiše spletni naslov, npr. https://www.example.com.
Brskalnik preveri, ali je naslov pravilen.

https://www.example.com

2 DNS – PREVOD IMENA V IP NASLOV

Brskalnik pošlje poizvedbo DNS strežniku, ki prevede domeno (npr. www.example.com) v IP naslov (npr. 93.184.216.34).
Rezultat se shrani v predpomnilnik.



3 TCP/IP – VZPOSTAVITEV POVEZAVE

Odjemalec vzpostavi povezavo do strežnika na IP naslovu preko protokola TCP.
Uporabi se določen vrata (npr. 443 za HTTPS).



4 NAT / ARP / MAC – LOKALNO OMREŽJE

Če smo v lokalnem omrežju, usmerjevalnik (NAT) prevede zasebni IP naslov v javni.
ARP poišče MAC naslov naslednjega hopa (npr. usmerjevalnika).



5 HTTP/HTTPS – PRENOS PODATKOV

Brskalnik pošlje zahtevo HTTP/HTTPS (npr. GET /).
Strežnik odgovori z vsebino (HTML, CSS, slike ...).
Podatki potujejo skozi omrežje v paketih.



6 PRIKAZ STRANI

Brskalnik prejete podatke razčleni, izvede HTML, CSS in JavaScript, ter prikaže spletno stran uporabniku.



FAZE KOMUNIKACIJE

1	Uporabnik vnese URL
2	DNS razreši ime
3	Vzpostavi se TCP povezava
4	Podatki se prenesejo
5	Stran se prikaže

UPORABLJENA OMREŽNA TEHNOLOGIJA

DNS	Prevodi domeno v IP naslov.
TCP/IP	Zagotavlja dostavo podatkov.
NAT	Prevod naslovov v omrežju.
ARP	Prevod IP v MAC naslov.
MAC	Fizični naslov omrežne kartice.
HTTP/HTTPS	Protokol za prenos spletnih vsebin.

DIAGNOSTIČNA ORODJA

ping	Preveri dosegljivost gostitelja.
nslookup	Preveri DNS zapise.
netstat	Prikaže mrežne povezave.
Wireshark	Analizira omrežni promet.

ENKAPSULACIJA PODATKOV SKOZI OMREŽNE SLOJE



VARNOST NA VSAKEM KORAKU

Preverjaj URL
Preveri pravilnost spletnega naslova.

Uporabi HTTPS
Šifrira komunikacijo med odjemalcem in strežnikom.

Zaupaj preverjenim strežnikom
Preveri digitalna potrdila.

Bodi pozoren na omrežje
Nevaren promet lahko razkrije podatke.

Znanje = zaščita
Razumevanje delovanja interneta je prvi korak do varne uporabe.

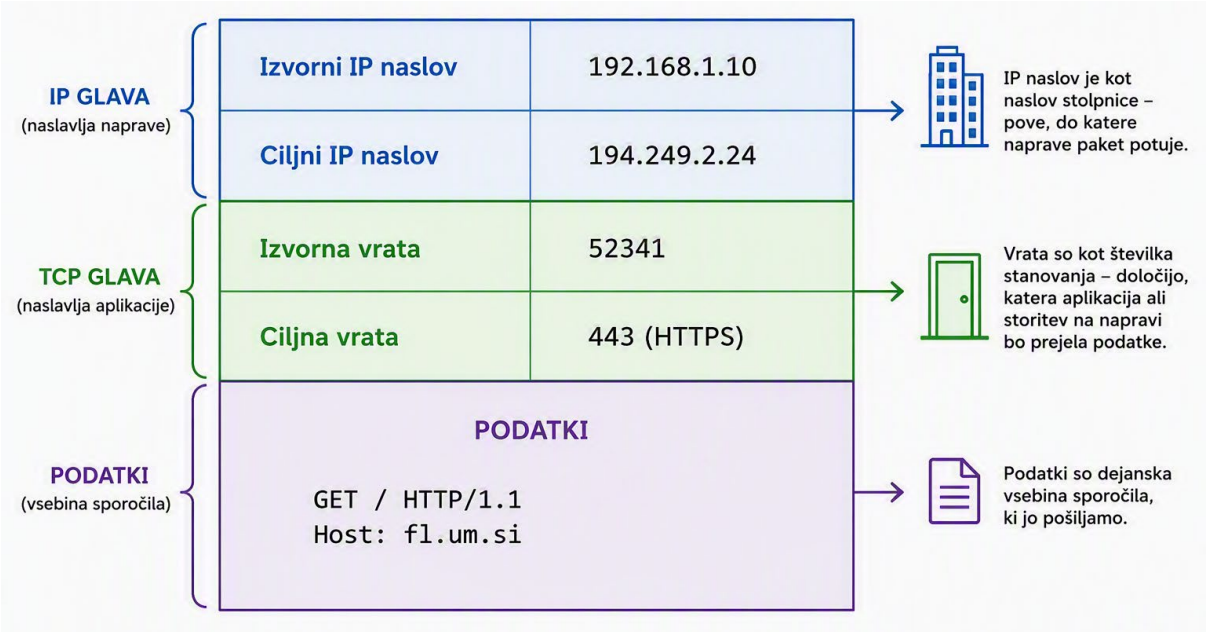
Univerzitetna založba
Univerze v Mariboru

1 Uvod

Vsaka naprava, ki je povezana v omrežje ali internet, ima svoj naslov IP (angl. *Internet Protocol Address*). Ta deluje podobno kot EMŠO ali davčna številka pri ljudeh, saj omogoča enolično prepoznavanje naprave v omrežju. Ko želimo poslati podatke določeni napravi, moramo poznati njen IP naslov. Nekatere naprave dobijo naslov IP le začasno, za čas svoje povezave v omrežje. To so na primer prenosni računalniki, mobilni telefoni in tablice, ki jim omrežna infrastruktura samodejno dodeli naslov. Druge naprave, predvsem strežniki in omrežna oprema, pa imajo pogosto stalne naslove IP, saj morajo biti uporabnikom vedno dosegljive na istem naslovu.

Za uspešno komunikacijo pa ni dovolj vedeti le, na kateri napravi se nahajajo podatki ali storitev. Na enem računalniku lahko hkrati deluje več različnih omrežnih aplikacij, na primer spletni strežnik, elektronska pošta ali podatkovna baza. Zato se poleg naslova IP uporabljajo tudi vrata (angl. *port numbers*), ki določajo, kateri aplikaciji so podatki namenjeni. Če si naslov IP predstavljamo kot naslov stolpnice, si lahko vrata predstavljamo kot številko posameznega stanovanja. Poštar mora najprej najti pravo stavbo, nato pa še pravo stanovanje. Podobno omrežni paket najprej prispe na pravilen IP naslov, vrata pa določijo, katera aplikacija bo prejela podatke.

Podatki po omrežju potujejo v obliki TCP/IP paketov. Paket poleg uporabniških podatkov vsebuje še različne kontrolne informacije, kot so izvorni in ciljni naslov IP ter izvorna in ciljna vrata. Te informacije omogočajo, da paket najde pravo pot do cilja in da ga na koncu prejme prava naprava ter prava aplikacija.



Slika 1: Poenostavljena zgradba TCP/IP paketa. IP naslova določata izvorno in ciljno napravo, številki vrat pa izvorno in ciljno aplikacijo oziroma storitev. Podatkovni del vsebuje vsebino sporočila, ki se prenaša po omrežju.

Ko v naslovno vrstico brskalnika vpišeš **https://fl.um.si** in pritisneš *Enter*, se v delčku sekunde sproži veriga dogodkov, ki bi bila brez orodij, kot je Wireshark, nevidna. Brskalnik pogleda v svoj predpomnilnik. Če strani ni, hitro razbere protokol *https*, domeno *fl.um.si* in zahtevo po varni seji. Računalnik mora najprej izvedeti, kam naj pošlje zahtevo, zato vpraša DNS: »Kje je fl.um.si?« Pretvornik (angl. *resolver*) mu v nekaj milisekundah odgovori: »Na naslovu 194.249.2.24.« Zdaj računalnik ve, komu je namenjen paket.

S temi informacijami brskalnik zgradi TCP zahtevo. V glavi TCP paketka zapiše izvorna in ciljna vrata (na tvoji napravi nekaj iz območja dinamičnih vrat in ciljna 443 za HTTPS), doda kontrolne podatke za zanesljiv prenos in pripravi paket za odhod. Ker si znotraj zasebnega omrežja, tvoj usmerjevalnik na poti izvede NAT: notranji naslov 192.168.x.x začasno preslika v javni naslov tvojega ponudnika, da bo paket prepoznan na internetu in da se bo odgovor znal vrniti prav do te naprave.

Preden paket zapusti lokalno omrežje, mora tvoj računalnik vedeti še fizični naslov, kamor ga bo poslal. S pomočjo ARP pošlje kratko vprašanje »Kdo je moj prehod?« in usmerjevalnik vrne svoj MAC naslov. Ethernet plast doda ta MAC kot cilj, kot tvoj izvor, nato vse skupaj pretvori v električne ali radijske signale in pošlje naprej k usmerjevalniku.

Signal zapusti tvojo napravo in ga ujamejo usmerjevalniki ponudnika. Ti na podlagi IP naslova 194.249.2.24 in svojih usmerjevalnih tabel odločajo o najprimernejši poti. Paket potuje skozi več vozlišč, kjer ga vsakokrat delno obdelajo in ponovno posredujejo, vse v le nekaj tisočinkah sekunde. Ko pride do strežnika na 194.249.2.24, ta prebere, da gre za HTTPS zahtevo, preveri (TCP/IP) glave in pošlje nazaj šifriran odgovor.

Ko odgovor prispe nazaj do tvojega usmerjevalnika, NAT vrne izvorno preslikavo na tvojo notranjo napravo, ARP poskrbi za pravilno lokalno dostavo, Ethernet okvirji odprejo pot do omrežne kartice, TCP pa potrdi prejetje. Brskalnik postopoma odstrani vse plasti: fizično, povezovalno, omrežno, transportno in varnostno, dokler ne ostane le HTML. Ta HTML brskalnik razčleni, naloži povezane slogovne datoteke in slike z dodatnimi zahtevami, sestavi stran in jo prikaže. Do trenutka, ko se na zaslonu pojavi domača stran fl.um.si, je minilo manj kot desetinka sekunde od tvojega pritiska na *Enter*. Za zaslonom pa so se med tem zgodile številne preslikave, usmerjanja, šifriranja in posredovanja, ki so skupaj omogočili ta kratek trenutek “čudeža” prikaza spletne strani.

Univerzitetna založba
Univerze v Mariboru

2 Faze poteka komunikacije od URL do prikaza spletne strani

Ko uporabnik v brskalnik vpiše spletni naslov, se v ozadju sproži zapleten niz omrežnih postopkov, ki se odvijejo v nekaj milisekundah, a omogočijo, da se želeni spletni vir prikaže na zaslonu. Brskalnik najprej razčleni vneseni URL, preveri lokalne zapise in izvede poizvedbo v sistem DNS, da pridobi ustrezen IP naslov strežnika. Nato se vzpostavi povezava prek protokolov TCP in IP ter, če gre za varno sejo, tudi TLS, s čimer se zagotovi zanesljiv in šifriran prenos podatkov. Na poti med odjemalcem in strežnikom sodelujejo številni omrežni mehanizmi, kot so NAT, ARP in usmerjanje, ki skrbijo, da paket podatkov najde pravo pot do cilja in se odgovor pravilno vrne. Ko brskalnik prejme odziv strežnika, odstrani omrežne ovoje (deenkapsulacija), razčleni vsebino HTML, naloži slogovne datoteke, slike in skripte ter jih predstavi uporabniku kot celovito spletno stran. Vse to se zgodi v manj kot sekundi. Rezultat pa je na videz preprost prikaz strani, ki ga omogoča natančno usklajeno delovanje številnih protokolov in tehnologij v ozadju.

1. Brskalnik razčleni naslov

- Uporabnik vnese https://fl.um.si/.
- Brskalnik razbije naslov na dele:
  - **protokol:** https,
  - **domena:** fl.um.si,
  - **Pot / datoteka:** / .
- Odloči se, da bo uporabil TCP in port 443 (ker gre za HTTPS).

2. Preverjanje predpomnilnika in lokalnih zapisov

- Brskalnik najprej pogleda, ali ima že **predpomnjeno kopijo IP naslova** za to domeno.
- Če je nima, preveri **lokalno datoteko hosts** – ali je domena tam ročno zapisana (npr. za razvojne ali testne namene).
- Če ne, nadaljuje poizvedbo o IP naslovu na DNS.

3. DNS – pretvorba domene v IP naslov

- Računalnik pošlje **DNS poizvedbo** (UDP port 53) lokalnemu DNS strežniku.
- Če ta ne pozna odgovora, poizvedba potuje k višjim strežnikom (root → .si → um.si).
- Rezultat: domena fl.um.si se pretvori v **IP naslov** (npr. 194.249.2.24).
- IP naslov se začasno shrani v lokalni DNS cache za hitrejše prihodnje dostope.

4. Priprava TCP povezave

- Brskalnik mora vzpostaviti povezavo s strežnikom na IP naslovu 194.249.2.24, vrata (port) 443.
- TCP povezava poteka s **tristopenjskim rokovanjem (angl. *3-way handshake*):**
  1. **SYN** – odjemalec pošlje zahtevo za vzpostavitev seje,
  2. **SYN-ACK** – strežnik potrdi sprejem,
  3. **ACK** – odjemalec potrdi in povezava je vzpostavljena.
- V tem trenutku je povezava pripravljena za varno izmenjavo podatkov.

5. TLS – vzpostavitev šifrirane seje (HTTPS)

- Ker gre za https, sledi **TLS handshake**:
  - strežnik pošlje svoj **digitalni certifikat** (izdan s strani CA)
  - brskalnik preveri, ali je certifikat veljaven in domena ustreza,
  - odjemalec in strežnik se dogovorita o **šifrirnih algoritmih** in ustvarita **sejni ključ**.
- Od tega trenutka naprej je komunikacija **šifrirana** (zaupnost in integriteta).

6. Pošiljanje HTTP zahteve

- Brskalnik pošlje prvo **HTTP zahtevo**:
  - GET / HTTP/1.1,
  - Host: fl.um.si,
  - User-Agent: Chrome/141.0,
  - Accept: text/html .
- Zahteva se ovije v TCP segment, ta v IP paket, in končno v Ethernet okvir.

7. Določitev fizičnega naslova – ARP

- Če je strežnik zunaj lokalnega omrežja, mora paket najprej do **privzetega prehoda (gateway)**.
- Računalnik pošlje **ARP poizvedbo**: "Kdo ima IP 192.168.1.1?".
- Usmerjevalnik odgovori s svojim **MAC naslovom**, ki se uporabi v Ethernet glavi.

8. NAT – preslikava naslovov (če gre skozi usmerjevalnik)

- Domači ali službeni usmerjevalnik uporabi **NAT (angl. *Network Address Translation*)**:
  - Zasebni naslov (npr. 192.168.1.50) se preslika v javni naslov (npr. 84.255.10.12).
  - V NAT tabeli se shrani zapis, da zna usmerjevalnik odgovor vrniti pravi notranji napravi.

9. Prenos skozi internet

- Paket potuje prek **več usmerjevalnikov** (hopov).
- Vsak usmerjevalnik:
  - prebere IP glavo,
  - zmanjša TTL (angl. *Time To Live*),
  - prepiše MAC naslov (naslednji hop),
  - pošlje naprej proti cilju.
- To je **usmerjanje** (angl. *routing*).

10. Strežnik sprejme zahtevo

- Na strežniku 194.249.2.24 posluša proces (npr. Apache ali Nginx) na portu 443.
- Prejme zahtevo GET / in pripravi odgovor:

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: ...
```

- Vključi HTML dokument, CSS, slike, JavaScript itd.

11. Vrnitev odgovora

- Odgovor potuje nazaj po isti poti:
  - IP naslov in vrata se zamenjata (cilj → vir),
  - NAT pretvori javni naslov nazaj v notranjega,
  - ARP zagotovi lokalno dostavo.
- TCP potrdi prejem z **ACK** paketom.

12. Brskalnik prejme in obdela vsebino

- Brskalnik odstrani vse plasti (deenkapsulacija): Ethernet → IP → TCP → TLS → HTTP.
- Prebere vsebino HTML in začne **upodabljati** spletno stran.
- Za vsako dodatno vsebino (slike, CSS, JS) pošlje nove HTTP(S) zahteve.

13. Izris strani

- Brskalnik sestavi **DOM (angl. *Document Object Model*)**.
- Požene JavaScript, naloži stile in slike.
- Na zaslonu se prikaže celotna spletna stran.

14. Časovni okvir

- Celoten proces od pritiska na Enter do prikaza prve vsebine traja:
  - ~50–150 ms v lokalnem omrežju,
  - ~200–500 ms pri tipični internetni povezavi.

15. Povzetek po plasteh (OSI model)

Tabela 1

Sloj	Protokol / Naloga
7. Aplikacijski	HTTP(S) – zahteva in odgovor
6. Predstavitveni	TLS – šifriranje in certifikati
4. Transportni	TCP – zanesljiv prenos, vrata 443
3. Omrežni	IP – usmerjanje paketov
2. Povezovalni	Ethernet – MAC naslovi, okvirji
1. Fizični	Električni / optični / radijski signal

Univerzitetna založba
Univerze v Mariboru

3 URL – naslov spletnega vira

3.1 Kaj je URL

URL (angl. *Uniform Resource Locator*) je spletni naslov, s katerim določimo, *kje* se nahaja določen vir (npr. spletna stran, slika, dokument) in *kako* naj ga brskalnik pridobi (Berners-Lee idr., 1994).

Vsakič, ko nekaj vpišemo v naslovno vrstico brskalnika, dejansko uporabljamo URL.

3.2 Sestava URL

URL ima več delov:

```
protokol://domena/pot/datoteka.html?parametri#sidro
```

primer: https://fl.um.si/studij/index.html?id=123#kontakt

Tabela 2

Del	Ime	Pomen
https://	Protokol	Določa, kako se vzpostavi povezava s strežnikom (npr. HTTP, HTTPS, FTP).
fl.um.si	Domena	Ime strežnika, kjer je vsebina shranjena. Domena je povezana z IP naslovom prek DNS.
/studij/	Pot (path)	Lokacija datoteke ali strani na strežniku.
index.html	Datoteka	Datoteka.
?id=123	Parameter (query string)	Podatki (parametri), ki jih brskalnik pošlje strežniku za obdelavo (ki jih strežnik uporabi npr. za iskanje, filtriranje, etc).
#kontakt	Sidro (anchor)	Skok na določen del strani (oznako znotraj dokumenta).

3.3 Protokoli v URL-jih

Najpogosteje uporabljeni protokoli so:

Tabela 3

Protokol	Pomen	Vrata
http://	Nešifriran prenos spletnih strani	80
https://	Šifriran prenos (TLS/SSL)	443
ftp://	Prenos datotek	21
file://	Dostop do lokalnih datotek	–

3.4 Kako brskalnik razume URL

Ko uporabnik vpiše npr.

https://fl.um.si,

brskalnik najprej:

1. prepozna, da gre za **HTTPS** (zato bo uporabil TCP vrata 443),
2. iz domene fl.um.si poskusi pridobiti **IP naslov** s pomočjo DNS,
3. pripravi **zahtevo (HTTP request)**, ki bo poslana strežniku.

3.5 Pomen za logistiko

URL (angl. *Uniform Resource Locator*) je standardiziran način naslavljanja spletnih virov, ki omogoča, da informacijski sistemi, aplikacije in uporabniki dostopajo do specifičnih vsebin, storitev ali podatkov na omrežju.

V logističnem okolju so URL naslovi nepogrešljivi za delovanje:

- **spletnih aplikacij** (npr. portali za naročila, sledenje pošiljk, e-računi),
- **API-jev** med informacijskimi sistemi (npr. WMS, TMS, ERP),
- **komunikacijskih storitev** (npr. FTP strežniki, REST klici, oblačne storitve),
- **infrastruktur IoT** (npr. senzorji, pametne etikete, kamere, AGV-ji).

Ker se skoraj vse storitve v digitalni logistiki izvajajo prek spletnih naslovov, je pravilno oblikovan in varen URL temelj razpoložljivosti, integracije in sledljivosti informacij.

3.6 Zakaj je to pomembno v praksi

Vsaka aplikacija ali storitev v logistiki uporablja URL za povezavo z drugimi sistemi – napačno zapisan, napačno preusmerjen ali kompromitiran URL lahko povzroči:

- nedostopnost spletnih portalov za partnerje ali stranke,
- neuspešno sinhronizacijo naročil med ERP in WMS,
- nepravilno usmerjanje podatkov na napačne strežnike,
- varnostne incidente zaradi phishinga ali zlonamernih preusmeritev.

Praktični primeri:

- Če API za sledenje pošiljk (https://api.dpd.si/v1/track) ne deluje ali se napačno preusmeri, se podatki o statusu dostave ne osvežujejo.
- Če spletna aplikacija uporablja nešifriran URL (http:// namesto https://), lahko napadalec prestreže uporabniške podatke.
- Če je URL napačno zapisan v konfiguraciji tiskalniškega strežnika (npr. ftp://192.168.1.250/labels), sistem ne bo mogel tiskati oznak.

3.7 Priporočila za logistična okolja

- **Vedno uporabljaj varne povezave (HTTPS)** — vsi logistični portali, API-ji in strežniki morajo uporabljati TLS šifriranje.
- **Redno preverjaj veljavnost certifikatov** — potekli ali napačni certifikati povzročajo prekinjene seje in izgubo zaupanja.
- **Uporabljaj stalne (angl. *canonical*) URL-je** — za aplikacije in dokumentacijo uporabljaj dosledno strukturo naslovov (npr. https://wms.company.si/orders).
- **Uporabi ustrezne kode preusmeritev (301, 302)** pri spremembi naslovov, da se povezave ohranijo delujoče.
- **Loči okolja (produkcija / test / razvoj)** z jasnimi URL-ji, npr. https://api-test.logistics.si → prepreči zamenjavo okolij.
- **Spremljaj URL dostopnost in odzivnost** (health-check) za ključne logistične storitve (WMS, TMS, ERP, EDI).
- **Centraliziraj konfiguracijo URL-jev** v sistemih — da se ob spremembi domene ali IP-ja izvede samodejna posodobitev.

3.8 Varnostni vidiki

URL je pogosto izkoriščen v napadih, ki ciljajo na uporabnike ali sisteme:

- **Spletno ribarjenje (angl. phishing)**— zlonamerni URL-ji, ki posnemajo legitimne portale (npr. logistics-portal.si-login.com).
- **Zloraba tipkarskih napak (angl. typosquatting)** — napake v črkovanju domen (npr. dhl-s1.com namesto dhl.si).
- **Zlonamerne preusmeritve (angl. *open redirect*)** — uporabnik je preusmerjen na nevarno spletno mesto.
- **Injekcije v URL parametrih** — napadi, kot so SQLi ali XSS (npr. https://portal.si/login?user=<script>).
- **Napačna uporaba HTTP metod** (GET namesto POST) lahko razkrije občutljive podatke v naslovni vrstici.

Za zaščito:

- uporabljaj **HTTPS in validirane certifikate**,
- preverjaj **vhodne parametre URL** (input validation),
- omeji **preusmeritve** na dovoljene domene,
- redno preverjaj **dnevnike dostopov** (URL patterns) v SIEM orodju in
- izobražuj uporabnike o **prepoznavanju sumljivih URL-jev**.

3.9 Primer

Če bi URL https://logistika.um.si/predmeti/vaje.html razstavili na posamezne dele:

- **protokol:** https,
- **domena:** logistika.um.si,
- **pot:** /predmeti/vaje.html in
- **vrata:** 443 (privzeto za HTTPS).

3.10 Vaja 1 – Prepoznaj dele URL-ja

Zapiši, katere dele imajo naslednji URL-ji:

1. https://www.gov.si/novice/varnost.html
2. http://localhost/test/index.html
3. https://shop.example.com/cart.php?item=7&color=blue

Dopolni tabelo:

URL	Protokol	Domena	Pot	Parameter

3.11 Vaja 2 – Praktični preizkus

1. Odpri brskalnik in v naslov vpiši:
   https://validator.w3.org/
2. Nato pritisni **F12** → zavihek **Network**.
   - Opazuj, kateri **URL** je poslan.
   - Zapiši celoten naslov, ki se pojavi v stolpcu "Name" ali "Request URL".

3. Klikni posamezno vrstico in preveri:
   - protokol: HTTP ali HTTPS?
   - vrata (port): 443 ali 80?

- parameter: ali vsebuje ? v naslovu?

3.12 Povzetek

Tabela 4

Pojem	Pomen
URL	Naslov spletnega vira (lokacija in način dostopa)
Protokol	Določa, kako poteka komunikacija
Domena	Ime strežnika (pretvori se v IP naslov)
Pot	Lokacija datoteke na strežniku
Parameter / sidro	Dodatne informacije za prikaz ali obdelavo

Univerzitetna založba
Univerze v Mariboru

4 DNS – Domenski sistem imen

4.1 Kaj je DNS

DNS (angl. *Domain Name System*) pretvarja človeško berljiva imena (npr. www.fl.um.si) v IP naslove (npr. 193.77.12.100) (Mockapetris, 1987a, 1987b).

Je "telefonski imenik interneta" — brez DNS večina storitev (HTTP, SMTP, FTP …) sploh ne deluje.

DNS poizvedbe so tudi pomemben **vektor napadov** (phishing, zastrupitev, zlorabe poddomen), zato je razumevanje preverjanja DNS ključnega pomena za varnostno ozaveščenost.

4.2 Kako deluje DNS?

Ko v brskalnik vpišemo npr. https://fl.um.si se sproži postopek iskanja IP naslova:

1. **Preverjanje lokalnega predpomnilnika (cache)** – računalnik najprej preveri, ali že pozna IP naslov za domeno.
2. **Poizvedba pri DNS strežniku** – če naslova še nima, pošlje poizvedbo (DNS query) najbližjemu DNS strežniku (običajno ponudnika interneta).
3. **Rekurzivna poizvedba** – če ta strežnik ne ve, kje je domena, vpraša višje ravni DNS (npr. *.si*, nato *um.si*).
4. **Odgovor (DNS response)** – strežnik vrne IP naslov in brskalnik lahko nadaljuje komunikacijo s strežnikom prek TCP/IP.

4.3 Osnovni zapisi v DNS

DNS vsebuje različne **zapise (angl. *records*)**, ki določajo, katera informacija je povezana z domeno.

Tabela 5

Vrsta zapisa	Pomen	Primer
A	IPv4 naslov	www.um.si → 164.8.100.110
AAAA	IPv6 naslov	www.um.si → 2001:1470:fffd::87
MX	Poštni strežnik	um-si.mail.protection.outlook.com
CNAME	Kanonično ime (alias)	primary name server = dorf21.uni-mb.si
NS	Strežnik imen	ns1.arnes.si
PTR	Obratna poizvedba (reverse lookup)	164.8.100.110→ www.um.si
TXT	Besedilni podatki (npr. SPF, DKIM, verifikacije)	v=spf1 include:spf.protection.outlook.com -all

4.4 Primer poizvedbe

Odpri ukazno vrstico / terminal

Windows

Pritisni **Win + R** → vpiši cmd → Enter

Linux / macOS

Odpri **Terminal**

Osnovno preverjanje DNS z nslookup

Primer:

```
nslookup www.nlb.si
```

Primer izpisa:

```
Server:  resolver1.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.nlb.si
Address: 193.77.12.100
```

Pomembno:

- Server: ti pove, **kateri DNS strežnik uporabljaš**.
- Address: je IP naslov, ki ga domena vrača.

Če domena kaže na sumljiv IP naslov (npr. v tujini ali neustrezen ASN), je to lahko znak zlorabe (DNS hijacking ali phishing).

Preveri e-poštne (MX) zapise

Če preverjaš legitimnost e-pošte, je koristno pogledati **MX zapise** (Mail eXchanger):

```
nslookup -type=mx nlb.si
```

Primer:

```
nlb.si      MX preference = 10, mail exchanger = mail.nlb.si
```

Če MX kaže na čudne zunanje strežnike (npr. mail.wixsite.com), je to opozorilni znak.

Preveri SPF, DKIM in DMARC zapise (TXT)

SPF

```
nslookup -type=txt nlb.si
```

Primer:

```
"v=spf1 ip4:193.77.12.0/24 -all"
```

Ta SPF zapis pove, kateri IP naslovi smejo pošiljati e-pošto v imenu domene nlb.si.

DKIM / DMARC

Če poznaš selector, lahko preveriš DKIM:

```
nslookup -type=txt selector1._domainkey.nlb.si
```

DMARC:

```
nslookup -type=txt _dmarc.nlb.si
```

Primer:

```
"v=DMARC1; p=reject; rua=mailto:dmarc-reports@nlb.si"
```

Legitimen pošiljatelj bo imel pravilno nastavljene SPF, DKIM in DMARC zapise. Phishing domene jih pogosto nimajo ali so napačni.

Preveri povratno razreševanje (Reverse DNS)

Zelo uporabno za preverjanje legitimnosti IP naslovov.

Primer:

```
nslookup 193.77.12.100
```

Primer izpisa:

```
Name:    mail.nlb.si
Address: 193.77.12.100
```

Če reverse DNS **ne ustreza pričakovani domeni** ali je prazen, je to znak za previdnost.

(Napredno) Uporabi dig za podrobnejše poizvedbe *(Linux/macOS)*

```
dig www.nlb.si
dig MX nlb.si
dig TXT nlb.si
```

Dig izpiše celoten DNS odgovor vključno z TTL, strežniki, authority sekcijo itd. Odlično za naprednejšo analizo (npr. preverjanje cache poisoning).

Znaki sumljivih DNS zapisov

Tabela 6

Kaj preveriti	Sumljiv primer
IP naslov	kaže na nenavadno lokacijo ali oblak brez povezave z organizacijo
MX zapisi	kažejo na tuje ali brezplačne poštne strežnike
SPF/DKIM/DMARC	manjkajo ali so nastavljeni površno
Reverse DNS	ni usklajen z domeno pošiljatelja
Poddomene	nenavadno kompleksne (npr. nlb2-61c66.firebaseapp.com)

4.5 Pomen za logistiko

DNS (angl. *Domain Name System*) je **osnovni mehanizem pretvorbe imen v IP naslove**, ki omogoča delovanje skoraj vseh aplikacij v logističnih informacijskih sistemih.

Predstavlja **"imenik digitalne infrastrukture"**, saj omogoča, da naprave, aplikacije in storitve med seboj komunicirajo prek razumljivih imen (npr. *wms.logistics.local*) namesto IP številk.
V logističnih omrežjih je DNS **ključna storitev za razpoložljivost, integracijo in varnost**, saj vpliva na delovanje skladiščnih sistemov, transportnih povezav, poštnih strežnikov in oblačnih aplikacij.

1. Zanesljivo delovanje logističnih informacijskih sistemov

- Vsi sodobni sistemi (WMS, ERP, TMS) uporabljajo DNS za dostop do strežnikov, baz in API-jev.
- Če DNS odpove ali napačno razrešuje imena, se seje ne vzpostavijo, kar lahko pomeni prekinitev procesov (npr. komisioniranje, izdaja nalepk, potrjevanje dobavnic).
- DNS zagotavlja enotno upravljanje povezav — spremembe IP naslovov se odrazijo brez ročnega poseganja v odjemalce.

2. Optimizacija povezljivosti in upravljanja naprav

- Logistične naprave (terminali, tiskalniki, tehtnice, AGV roboti, kamere) komunicirajo prek DNS imen, kar omogoča centralizirano upravljanje.
- Z DNS lahko nadomestimo statične IP nastavitve, kar poenostavi menjavo ali nadgradnjo naprav.
- Vzpostavitev lokalnega *caching resolverja* v skladišču zmanjša zakasnitve in izboljša odzivnost sistemov.

3. Podpora elektronski pošti in komunikacijskim sistemom

- MX, SPF, DKIM in DMARC zapisi določajo, kateri strežniki so pooblaščeni za pošiljanje pošte v imenu organizacije.
- Pravilno nastavljeni zapisi preprečujejo zlorabe (phishing, spoofing) in izboljšajo dostavljivost sporočil (naročila, potrdila, obvestila).
- V primeru napak v teh zapisih lahko logistične aplikacije izgubijo sposobnost samodejnega pošiljanja e-poštnih potrditev ali poročil.

4. Sledenje, portali in zunanje integracije

- Večina integracij s prevozniki (DHL, DPD, GLS) uporablja FQDN naslove API-jev za izmenjavo podatkov o pošiljkah.
- Če DNS vrne napačen IP ali ne deluje, se prekine izmenjava podatkov — kar povzroči zastoje pri odpremah in sledenju.
- DNS podpira *geo-distribucijo* (prek CDN in geo-DNS), kar zagotavlja hitrejši odziv pri dostopanju do globalnih storitev.

5. Varnostni mehanizmi in obramba pred zlorabami

- DNS je pogosto prva točka preverjanja legitimnosti domen in strežnikov.
- Z ukazi nslookup, dig ali z orodji SIEM je mogoče hitro prepoznati sumljive zapise (npr. napačen IP, lažen MX ali nenavadne poddomene).
- Implementacija *DNSSEC* zagotavlja preverjanje pristnosti DNS odgovorov in preprečuje zastrupitev predpomnilnika (angl. *cache poisoning*).
- Uporaba zaščitenih DNS storitev (angl. *sinkhole DNS*, *threat intelligence filtering*) preprečuje dostop do znanih zlonamernih domen in C2 strežnikov.

4.6 Zakaj je to pomembno v praksi

V praksi lahko že manjše napake v DNS povzročijo velike operativne motnje:

- WMS terminali ne najdejo strežnika → ustavitev skladiščnega dela.
- TMS API ne more povezati prevozniškega strežnika → zadržana odpremna dokumentacija.
- E-poštni strežniki zaradi napačnih MX ali SPF zapisov ne dostavijo obvestil o dobavah.
- Zunanji ponudniki SaaS niso dosegljivi zaradi nepravilno nastavljenih CNAME ali TTL parametrov.

Z vidika varnosti so pogoste zlorabe:

- **Phishing domene**, ki posnemajo portale partnerjev ali prevoznikov,
- **DNS hijacking**, kjer gre za preusmerjanje domen na lažne IP naslove,
- **DNS tunneling**, ki pomeni uporabo DNS kanalov za iznos podatkov ali C2 komunikacijo malware-a.

4.7 Priporočila za logistična okolja

- Vzpostavi **dva neodvisna rekurzivna resolverja** (npr. lokalni + anycast) za redundanco.
- Uporabi **split-horizon DNS** — ločene zapise za notranje (npr. wms.internal.lan) in zunanje domene.
- Omogoči **DNSSEC validacijo** in redno preverjaj SPF, DKIM in DMARC zapise.
- Dovoli odjemalcem poizvedbe le do lastnih resolverjev, blokiraj neposreden odhodni promet UDP/TCP 53 proti internetu.
- Nastavi **kratke TTL** vrednosti za migracije ali selitve API-jev, daljše TTL za stabilne zapise.
- Spremljaj DNS dnevnike v **SIEM** in išči anomalije (npr. dolge poddomene, nenavadne TLD-je, neznane MX strežnike).
- Vzpostavi **nadzor zdravja (angl. *health-check*)** za kritične FQDN naslove (WMS, TMS, ERP, identitetne storitve).
- Zagotovi **rezervne DNS strežnike** v ločenih VLAN-ih ali energijskih segmentih.

DNS je **temelj zanesljive komunikacije in varnega delovanja digitalne logistične infrastrukture**.

Omogoča učinkovito povezovanje vseh komponent, od terminalov in strežnikov do oblačnih platform, in hkrati predstavlja **prvo linijo obrambe** pred številnimi napadi. Njegovo pravilno upravljanje in spremljanje neposredno vplivata na **operativno stabilnost, varnost in pretočnost informacij** v celotni oskrbovalni verigi.

4.8 Varnostni vidik

DNS je pogosto **prva točka preverjanja legitimnosti domene**:

- phishing uporablja poddomene, nove registracije, napačne IP-je, lažne MX zapise, itd.,
- z osnovnimi ukazi nslookup in dig lahko hitro odkriješ številne poskuse zavajanja.

4.9 Tipične vaje / praktični koraki

1. Izvedi nslookup www.example.com in preveri IP naslov ter DNS strežnik.
2. Preveri MX zapise (nslookup -type=mx domena.si) in identificiraj poštne strežnike.
3. Preglej SPF, DKIM in DMARC zapise (nslookup -type=txt domena.si, _dmarc.domena.si).
4. Izvedi *reverse DNS* poizvedbo (nslookup <IP>) in preveri ujemanje imen.
5. Analiziraj rezultate dig za TTL in authority sekcije.
6. Prepoznaj sumljive zapise (npr. tuji MX, nenavaden IP, manjkajoč DMARC).
7. Pripravi predlog izboljšav DNS konfiguracije (redundanca, validacija, TTL politika).

4.10 Vaje

Vaja 1 – Prepoznaj dele DNS odgovora

Zapiši, kaj pomenijo naslednji deli odgovora DNS:

Element	Opis
Server	
Address	
Name	
Address (v drugi vrstici)	

Vaja 2 – Praktični preizkus

1. Odpri **ukazno vrstico (cmd)** ali **PowerShell**.
2. Izvedi ukaz:
   nslookup www.gov.si
3. Nato poskusi še:
   nslookup -type=mx um.si
4. Zapiši rezultate:
   - IP naslov:
   - Poštni strežnik (MX):
   - Ali obstaja CNAME zapis?

Vaja 3 – Preverjanje spletnih domen

Odpri spletno stran:

https://dnschecker.org

1. Vpiši domeno: um.si
2. Izberi zapis: **A**
3. Opazuj, kateri IP naslovi so prikazani iz različnih držav.
4. Preveri tudi zapis **MX** in **TXT** ter zapiši ugotovitve.

4.11 Povzetek postopka DNS preverjanja

Tabela 7

Korak	Ukaz	Namen
1	nslookup domena	Preveri IP naslov domene
2	nslookup -type=mx domena	Preveri poštne strežnike
3	nslookup -type=txt domena	Preveri SPF / DKIM / DMARC
4	nslookup <IP>	Reverse DNS preverjanje
5	dig ... (napredno)	Podrobne DNS analize

Univerzitetna založba
Univerze v Mariboru

5 Hosts datoteka

Preden računalnik pošlje poizvedbo na DNS strežnik, **najprej preveri lokalno datoteko hosts**.

Ta datoteka omogoča **ročno preslikavo domen na IP naslove** — uporablja se za testiranje, razvoj ali blokiranje dostopa do določenih spletnih strani.

Kje se nahaja?

- **Windows:**

```
C:\Windows\System32\drivers\etc\hosts
```

- **Linux / macOS:**

```
/etc/hosts
```

- **Primer vsebine datoteke**

```
# Komentarji se začnejo z #
127.0.0.1          localhost
192.168.1.10       intranet.podjetje.si
93.184.216.34      www.example.com
0.0.0.0            reklame.splet.com
```

Tabela 8

Vrstica	Pomen
127.0.0.1 localhost	Določa lokalni računalnik (loopback naslov)
192.168.1.10 intranet.podjetje.si	Domena znotraj lokalnega omrežja
93.184.216.34 www.example.com	Ročna preslikava zunanjega spletnega mesta
0.0.0.0 reklame.splet.com	Onemogoči dostop do določene strani (blokada)



Vaja 1 – Preizkus z datoteko hosts

Opozorilo: datoteko hosts lahko urejaš le z administratorskimi pravicami.

1. Odpri **Notepad kot skrbnik** (Run as Administrator).
2. Odpri datoteko:

```
C:\Windows\System32\drivers\etc\hosts
```

3. Dodaj vrstico:

```
127.0.0.1   testna-stran.si
```

4. Shrani datoteko.
5. Odpri brskalnik in vpiši:
6. http://testna-stran.si
   — brskalnik bo poskusil dostopati do *lokalnega računalnika* (ne na internet).
7. Po testu **vrstico izbriši ali zakomentiraj**, da se izogneš zmedi pri DNS poizvedbah.

5.1 Povzetek

Tabela 9

Pojem	Pomen
Hosts datoteka	Lokalna datoteka za ročno preslikavo domen na IP naslove
Prednost	Ima prednost pred DNS poizvedbo
Namen	Testiranje, razvoj, blokada dostopa
Lokacija	C:\Windows\System32\drivers\etc\hosts (Windows)
Urejanje	Možno le s skrbniškimi pravicami

Univerzitetna založba
Univerze v Mariboru

6 IPV4 naslovni prostor

IPv4 (angl. *Internet Protocol version 4*) je najstarejši in še vedno najbolj razširjen naslovni sistem v računalniških omrežjih. Razvit je bil konec 70. let prejšnjega stoletja in je postal temeljni mehanizem za usmerjanje prometa v internetu. Vsaki napravi omogoča, da dobi enoličen naslov, preko katerega lahko pošilja in prejema podatke.

Zaradi zgodovinske vloge in široke uporabe je poznavanje IPv4 nujno za razumevanje sodobnih omrežij, tudi če se IPv6 (Deering in Hinden, 2017) postopoma uveljavlja kot njegov naslednik.

6.1 Dolžina in zapis IPv4 naslovov

IPv4 uporablja **32-bitne naslove**, ki so zapisani v **štirih oktetih** (vsak po 8 bitov) (Postel, 1981b; Touch, 2013).

Za lažje branje so zapisani v **decimalni obliki**, posamezni okteti pa so ločeni s pikami.

Primer IPv4 naslova:

```
192.168.10.25
```

Vsak oktet lahko ima vrednost med 0 in 255.

Skupno število možnih IPv4 naslovov je: 2^{32} kar pomeni približno 4,3 milijarde naslovov.

6.2 Zgodovinska razdelitev na razrede (A–E)

Sprva je bil IPv4 naslovni prostor razdeljen na **naslovne razrede**, ki so določali razmerje med omrežnim in gostiteljskim delom. Ta sistem je bil enostaven, a tog, zato ga je pozneje nadomestil CIDR. Kljub temu je razredna delitev pomembna za razumevanje razvoja interneta.

Tabela 10

Razred	Prvi oktet	Maska omrežja	Omrežni del	Gostiteljski del	Št. omrežij	Št. gostiteljev / omrežje	Namen
A	0–127	255.0.0.0 (/8)	8 bitov	24 bitov	128	≈ 16 milijonov	zelo velika omrežja
B	128–191	255.255.0.0 (/16)	16 bitov	16 bitov	16.384	≈ 65.000	srednje velika omrežja
C	192–223	255.255.255.0 (/24)	24 bitov	8 bitov	2 milijona	254	majhna omrežja
D	224–239	–	–	–	–	–	multicast
E	240–255	–	–	–	–	–	rezervirano za raziskave

Opomba: Razredi D in E se ne uporabljajo za običajno naslavljanje gostiteljev. Razred D je namenjen multicast prometu, razred E pa eksperimentalnim namenom.

Število uporabnih gostiteljskih naslovov je vedno 2^(32 - maska) – 2, saj sta prvi naslov rezerviran za omrežje, zadnji pa za broadcast.

Rezervirani in posebni naslovi

Nekateri IPv4 naslovi imajo **posebne funkcije** in jih ne dodeljujemo napravam v običajnih omrežjih:

- **0.0.0.0**

Označuje "neznani" naslov ali privzeto pot. Uporablja se v konfiguracijah in pri dodeljevanju naslovov prek DHCP.

- **255.255.255.255**

Poseben **broadcast naslov**, s katerim se pošiljajo sporočila vsem napravam v lokalnem omrežju.

– **127.0.0.0/8 (npr. 127.0.0.1)**

Loopback naslov, ki predstavlja lokalno napravo. Uporablja se za testiranje omrežnega sklada (localhost).

– **169.254.0.0/16**

Samodejni zasebni naslov (*APIPA*), ki ga naprave prejmejo, če ni na voljo DHCP strežnika.

6.3 Tipične vaje / praktični koraki

1. Prepoznaj število bitov in bajtov v IPv4 naslovu.
2. Pretvori IPv4 naslov med decimalnim in binarnim zapisom.
3. Določi, kateremu naslovnemu razredu pripada IPv4 naslov.
4. Prepoznaj posebne IPv4 naslove (loopback, broadcast, APIPA).
5. Ocenjuj velikost IPv4 naslovnega prostora.
6. Razloži omejitve IPv4 naslovnega prostora in potrebo po učinkoviti porabi naslovov.

Vaja 1 – Koliko IPv4 naslovov obstaja?

IPv4 naslov je sestavljen iz štirih bajtov oziroma 32 bitov. Vsak bit lahko zavzame eno od dveh vrednosti: 0 ali 1.

Odgovori na vprašanja:

1. Koliko različnih kombinacij lahko ustvarimo z 32 biti?
2. Rezultat zapiši v obliki potence.
3. Koliko naslovov to predstavlja približno?
4. Ali se ti to število zdi veliko ali majhno glede na število naprav, povezanih v internet?

Vaja 2 – Pretvori IPv4 naslov v binarni zapis

Pretvori naslednji IPv4 naslov v binarno obliko:

```
192.168.10.25
```

Nato odgovori:

1. Koliko bitov vsebuje vsak oktet?
2. Koliko bitov vsebuje celoten IPv4 naslov?
3. Kateri zapis se ti zdi preglednejši: binarni ali decimalni?

Vaja 3 – Določi naslovni razred

Za naslednje IPv4 naslove določi naslovni razred (dopolni tabelo):

IPv4 naslov	Razred
10.5.25.1	
172.16.10.5	
192.168.1.25	
224.0.0.5	
245.10.10.10	

Vaja 4 – Posebni IPv4 naslovi

Za vsak naslov določi njegovo vlogo (dopolni tabelo):

IPv4 naslov	Vloga
127.0.0.1	
255.255.255.255	
169.254.12.88	
0.0.0.0	

Odgovori na vprašanja:

1. Kateri naslov predstavlja loopback?
2. Kateri naslov predstavlja broadcast?
3. Kateri naslov pripada območju APIPA?
4. Kdaj se uporablja naslov 0.0.0.0?



Vaja 5 – Razmislek

Odgovori na vprašanja:

1. Zakaj je IPv4 naslov sestavljen iz štirih oktetov?
2. Katera je glavna omejitev IPv4 naslovnega prostora?
3. Zakaj se je pojavila potreba po uvedbi IPv6?

6.4 Povzetek

IPv4 naslovni prostor je bil zasnovan kot enostaven sistem za zgodnji internet, a ima omejeno velikost in togost razredov. Uvedba CIDR je omogočila bolj racionalno uporabo naslovov, a kljub temu je razpoložljivih naslovov vedno manj, kar je spodbudilo prehod na IPv6. Dobro razumevanje IPv4 strukture, razredov, mask in posebnih naslovov je ključnega pomena za delo v sodobnih omrežjih.

Univerzitetna založba
Univerze v Mariboru

7 Zasebni, javni in posebni naslovi (IPv4)

Vsaka naprava v omrežju mora imeti enoličen IP naslov, da jo je mogoče prepoznati in ji dostaviti podatke. Ker pa je IPv4 naslovni prostor omejen, so se sčasoma oblikovale različne **vrste naslovov**, namenjene različnim vlogam in okoljem. Razumevanje teh razlik je bistveno za pravilno načrtovanje in delovanje lokalnih in globalnih omrežij.

IPv4 naslove delimo v tri osnovne skupine:

1. **javni naslovi** – uporabljajo se v internetu, morajo biti globalno enolični in so javno dosegljivi,
2. **zasebni naslovi** – namenjeni so uporabi v notranjih (lokalnih) omrežjih in niso neposredno dostopni iz interneta,
3. **posebni naslovi** – imajo določene rezervirane funkcije, npr. za testiranje, samodejno konfiguracijo ali multicast promet.

7.1 Javni naslovi

Javni IP naslovi so globalno enolični in omogočajo, da je naprava ali storitev dosegljiva prek interneta. Ti naslovi morajo biti usklajeno dodeljeni, da se ne pojavijo podvojitve.

Za dodeljevanje javnih naslovov skrbi organizacija **IANA** (angl. *Internet Assigned Numbers Authority*), ki razdeljuje naslovni prostor regionalnim registrarjem (**RIR**, angl. *Regional Internet Registries*). Ti so odgovorni za nadaljnjo delitev posameznim ponudnikom internetnih storitev (ISP) in organizacijam.

Glavni regionalni registrarji so:

- **RIPE NCC** – za Evropo, Bližnji vzhod in dele Azije,
- **ARIN** – za Severno Ameriko,
- **APNIC** – za Azijo in Pacifik,
- **LACNIC** – za Latinsko Ameriko,
- **AfriNIC** – za Afriko.

Javni naslovi so namenjeni neposredni komunikaciji prek interneta. Primer: 193.2.1.45 je javni naslov strežnika, dostopen z vsega sveta.

7.2 Zasebni naslovi (RFC 1918)

Zaradi omejenega števila javnih naslovov je bil uveden standard **RFC 1918** (Rekhter idr., 1996), ki določa obsege **zasebnih naslovov**. Ti naslovi so namenjeni uporabi znotraj organizacijskih ali domačih omrežij (LAN) in se **ne usmerjajo v javni internet**.

Tabela 11

Razred	Obseg naslovov	Maska / CIDR	Tipična uporaba
A	10.0.0.0 – 10.255.255.255	/8	velika interna omrežja
B	172.16.0.0 – 172.31.255.255	/12	srednje velika omrežja
C	192.168.0.0 – 192.168.255.255	/16	domača in manjša omrežja

Zasebni naslovi se pogosto uporabljajo v kombinaciji z **NAT** (angl. *Network Address Translation*), ki omogoča, da več notranjih naprav uporablja en sam javni naslov za dostop v internet. To je danes najpogostejša oblika naslavljanja v domačih in poslovnih omrežjih.

Primer uporabe zasebnih naslovov:

- terminal v skladišču ima naslov 192.168.10.25,
- preko NAT dostopa do javnega interneta prek skupnega zunanjega naslova podjetja, npr. 84.255.12.90.

Prednost zasebnih naslovov je, da jih lahko poljubno uporabimo znotraj organizacije, ne da bi jih bilo treba pridobiti od registrarjev.

Posebni naslovi

Nekateri IPv4 naslovi so **rezervirani za posebne funkcije** in se ne uporabljajo za običajno naslavljanje naprav.

Tabela 12

Naslov / Obseg	Namen	Opis
127.0.0.0/8	Loopback	Predstavlja lokalni računalnik (localhost). Uporablja se za testiranje omrežnega sklada. Najpogosteje uporabljen naslov je 127.0.0.1.
169.254.0.0/16	APIPA (Automatic Private IP Addressing)	Samodejni naslov, ki ga dodeli operacijski sistem, če DHCP ni na voljo. Omogoča osnovno komunikacijo znotraj istega segmenta.
224.0.0.0 – 239.255.255.255	Multicast	Namenjeni skupinski komunikaciji z več napravami hkrati.
0.0.0.0	Neznani ali privzeti naslov	Uporablja se pri inicializaciji omrežnih vmesnikov in v konfiguracijah kot "kateri koli naslov".
240.0.0.0 – 255.255.255.254	Rezervirano za prihodnjo rabo	Trenutno ni v uporabi za javno naslavljanje.

Ti naslovi imajo v omrežjih zelo specifično vlogo. Njihova napačna uporaba (npr. dodelitev 127.0.0.5 fizični napravi) lahko povzroči nedelujoče komunikacijske poti.

7.3 Tipične vaje / praktični koraki

1. Prikaži svoj IPv4 naslov z ukazom ipconfig (Windows) ali ip addr (Linux/macOS).
2. Ugotovi, ali je naslov javni, zasebni ali posebni naslov.
3. Prepoznaj zasebne naslovne prostore RFC 1918.
4. Primerjaj lokalni IP naslov in javni IP naslov svoje internetne povezave.
5. Prepoznaj posebne naslove, kot so loopback, APIPA in broadcast.
6. Določi omrežni in gostiteljski del naslova ob podani omrežni maski.
7. Izračunaj prvo in zadnjo uporabno številko v omrežju.
8. Razmisli, zakaj se v lokalnih omrežjih uporabljajo zasebni naslovi in NAT.

Vaja 1 – Prepoznaj zasebni IP naslov

Podani so naslednji naslovi (dopolni tabelo):

IPv4 naslov	Zasebni ali javni
10.0.5.77	
172.20.15.8	
192.168.10.25	
84.255.12.90	

Vaja 2 – Prepoznaj javni IP naslov

Podan je naslov:

```
84.255.12.90
```

Odgovori na vprašanja:

1. Ali je naslov javen ali zaseben?
2. Zakaj je lahko dosegljiv iz interneta?
3. Kdo dodeljuje javne IP naslove?
4. Zakaj organizacije pogosto uporabljajo NAT?

Vaja 3 – Poišči svoj lokalni IP naslov

Odpri ukazno vrstico in izvedi ukaz:

```
ipconfig
```

Odgovori na vprašanja:

1. Kakšen je tvoj IPv4 naslov?
2. V kateri naslovni prostor spada?

3. Ali gre za javni ali zasebni naslov?
4. Katera naprava v omrežju je privzeti prehod (angl. *Default Gateway*)?



Vaja 4 – Primerjaj lokalni in javni IP naslov

Preveri svoj lokalni naslov z ukazom:

```
ipconfig
```

Nato obišči spletno stran:

```
https://whatismyip.com
```

Odgovori na vprašanja:

1. Katera dva naslova si dobil?
2. Zakaj se razlikujeta?
3. Kateri naslov vidi spletni strežnik na internetu?
4. Katera tehnologija omogoča to preslikavo?



Vaja 5 – Posebni naslov: loopback

Podan je naslov:

```
127.0.0.1
```

Odgovori na vprašanja:

1. Kaj pomeni izraz loopback?
2. Kaj predstavlja naslov localhost?
3. Za kaj ga uporabljamo pri testiranju?



Vaja 6 – Posebni naslov: broadcast

Podan je naslov:

```
255.255.255.255
```

Odgovori na vprašanja:

1. Ali se ta naslov lahko dodeli računalniku?
2. Kaj pomeni izraz broadcast?
3. Kdaj se uporablja oddajanje vsem napravam v omrežju?



Vaja 7 – APIPA naslov

Podan je naslov:

```
169.254.12.88
```

Odgovori na vprašanja:

1. Ali gre za APIPA naslov?
2. Kaj pomeni kratica APIPA?
3. Kdaj računalnik samodejno prejme tak naslov?
4. Kaj to običajno pove o delovanju omrežja?



Vaja 8 – Omrežni in gostiteljski del naslova

Podan je naslov:

```
192.168.1.50
```

Omrežna maska:

```
255.255.255.0
```

Odgovori na vprašanja:

1. Kateri del predstavlja omrežje?
2. Kateri del predstavlja gostitelja?
3. Koliko naprav lahko naslovimo v takem omrežju?

Vaja 9 – Prva in zadnja uporabna IP številka

Podano je omrežje:

```
192.168.10.0/24
```

Odgovori na vprašanja:

1. Kateri naslov predstavlja omrežje?
2. Katera je prva uporabna IP številka?
3. Katera je zadnja uporabna IP številka?
4. Kateri naslov predstavlja broadcast?

Vaja 10 – Zakaj potrebujemo NAT?

Predstavljaj si podjetje s 500 računalniki.

Odgovori na vprašanja:

1. Ali bi vsak računalnik potreboval svoj javni IP naslov?
2. Kakšne težave bi to povzročilo?
3. Kako NAT pomaga pri reševanju tega problema?
4. Katere prednosti prinaša uporaba zasebnih naslovov?

7.4 Povzetek

- **Javni naslovi** so globalno enolični in omogočajo dostop prek interneta.
- **Zasebni naslovi** so namenjeni notranjim omrežjem in zahtevajo NAT za dostop do interneta.
- **Posebni naslovi** opravljajo specifične funkcije, ki omogočajo testiranje, samodejno konfiguracijo ali skupinsko komunikacijo.

Razlikovanje teh vrst naslovov je ključno za pravilno načrtovanje omrežij, odpravljanje napak in zagotavljanje varnega dostopa do storitev.

Univerzitetna založba
Univerze v Mariboru

8 ICMP

8.1 Kaj je ICMP?

ICMP (angl. *Internet Control Message Protocol*) je protokol za prenos **kontrolnih in diagnostičnih sporočil** v IP omrežjih (Postel, 1981a).

Uporablja se za preverjanje:

- dosegljivosti druge naprave,
- časa potovanja paketov (latenca),
- poti do cilja (routing).

ICMP sam **ne prenaša podatkov**, ampak **odzive** omrežnih naprav (npr. "Host unreachable", "Time exceeded").

Najbolj znana ukaza, ki uporabljata ICMP:

- ping
- tracert (Windows) / traceroute (Linux/macOS)

8.2 Preverjanje

Odpri ukazno vrstico / terminal

Windows

- Pritisni **Win + R** → vpiši cmd → Enter

Linux/macOS

- Odpri **Terminal**

Preveri lokalno povezavo (ping gateway)

Najprej preveri povezavo do privzetega prehoda (gateway), ki ga izveš z ipconfig ali ip addr.

Primer:

```
ping 192.168.0.1
```

Primer izpisa:

```
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
```

Pomembni elementi:

- **Reply from** → povezava je delujoča.
- **time=** → latenca v milisekundah (zelo nizka v LAN).
- **TTL (Time-To-Live)** → število preostalih skokov (vsak usmerjevalnik zmanjša za 1).

Če dobiš Request timed out ali Destination unreachable, je problem v povezavi, firewallu ali IP konfiguraciji.

Preveri zunanjo povezavo (ping domena)

Primer:

```
ping www.nlb.si
```

Primer izpisa:

```
Pinging www.nlb.si [193.77.12.100] with 32 bytes of data:
Reply from 193.77.12.100: bytes=32 time=25ms TTL=54
```

To preveri tri stvari naenkrat:

- delovanje **DNS** (pretvorba domene v IP),
- **lokalno omrežno povezavo,**
- **dostopnost zunanjega strežnika.**

Če DNS ne deluje, boš dobil napako:

```
Ping request could not find host www.nlb.si.
```

Če je IP dosegljiv, boš dobil odzive s časom in TTL.

8.3 Preveri pot do cilja – tracert / traceroute

Traceroute ti pokaže **vse vmesne usmerjevalnike (hop-e)**, skozi katere paket potuje do cilja.

Primer (Windows):

```
tracert www.nlb.si
```

Primer izpisa:

```
Tracing route to www.nlb.si [193.77.12.100]
over a maximum of 30 hops:

  1    2 ms    1 ms    1 ms  192.168.0.1
  2    11 ms   10 ms   12 ms 10.10.0.1
  3    15 ms   14 ms   13 ms  si-lj-isp-gw.isp.net [83.222.33.1]
  4    25 ms   24 ms   23 ms www.nlb.si [193.77.12.100]
```

Primer (Linux/macOS):

```
traceroute www.nlb.si
```

Pomembno:

- **Vsaka vrstica je en hop** → usmerjevalnik na poti.
- Lahko vidiš, kje pride do zakasnitev ali izpada.

– * * * pomeni, da usmerjevalnik ne vrača ICMP Time Exceeded (lahko firewall).

8.4 Dodatne možnosti ping

Preveri število poizvedb

```
ping -n 10 192.168.0.1   # Windows
ping -c 10 192.168.0.1   # Linux/macOS
```

Izvede 10 ICMP poizvedb in prikaže statistiko (uspešnost, povprečni čas, izgube).

8.5 Preveri velikost paketov

```
ping -l 1000 www.nlb.si   # Windows (1000 bajtov)
ping -s 1000 www.nlb.si   # Linux/macOS
```

Uporabno za preverjanje MTU ali zmogljivosti povezave.

8.6 Tipični rezultati in pomen

Tabela 13

Rezultat	Pomen
Odgovor + čas + TTL	Naprava je dosegljiva
Request timed out	Ni odziva – lahko filter, napaka ali izpad
Unknown host	DNS ne deluje
Destination unreachable	Napaka v IP poti ali gatewayu
TTL zelo nizek	Naprava daleč (veliko hopov) ali napačno konfiguriran TTL

8.7 Pomen za logistiko

ICMP (angl. *Internet Control Message Protocol*) ima v logističnih okoljih pomembno diagnostično in nadzorno vlogo, saj omogoča preverjanje dosegljivosti naprav, hitro zaznavanje motenj in analizo poti med logističnimi vozlišči, strežniki in zunanjimi sistemi. Uporablja se v vseh fazah delovanja logističnih informacijskih sistemov — od osnovne povezljivosti skladiščnih terminalov do nadzora delovanja mednarodnih transportnih omrežij.

1. Preverjanje dosegljivosti naprav in storitev

– ICMP omogoča preverjanje, ali so strežniki, terminali, tiskalniki, senzorji in druge naprave v omrežju dosegljive.

- Ukaza ping in tracert/traceroute omogočata hitro ugotavljanje, ali je težava v lokalnem omrežju, gatewayu ali zunanji povezavi.
- V skladiščih in distribucijskih centrih se ICMP uporablja za nadzor delovanja ključnih IP naprav (WMS strežniki, Wi-Fi dostopne točke, čitalniki kod).

2. Nadzor med-lokacijskih in WAN povezav

- Logistična infrastruktura pogosto povezuje več lokacij (npr. centralni ERP v Ljubljani in skladišča po Sloveniji ali tujini).
- Z ICMP je mogoče redno spremljati odzivne čase in izgube paketov med lokacijami.
- Traceroute omogoča prepoznavo, v kateri točki WAN povezave prihaja do zakasnitev ali prekinitev.

3. Podpora pri incidentnem odzivanju in diagnostiki

- Pri izpadih omrežja je ICMP osnovno orodje za ločevanje težav: lokalna napaka, napačna konfiguracija ali zunanji izpad.
- Če ping do gatewaya uspe, vendar ne do zunanjega strežnika, je težava v usmerjanju ali DNS.
- ICMP rezultati so pogosto prvi dokazni podatki, ki jih uporablja tehnična ekipa pri analizi dogodkov (v kombinaciji z logi iz SIEM ali požarnih zidov).

4. Podpora transportnim in oblačnim storitvam

- Sistemi za sledenje pošiljk, API-ji prevoznikov (DHL, GLS, UPS) in oblačne aplikacije zahtevajo stabilne povezave.
- Z ICMP testiranjem se redno preverja razpoložljivost teh zunanjih storitev in kakovost internetne povezave.
- Pri upočasnitvah ali izpadih ICMP pomaga hitro določiti, ali težava izvira znotraj organizacije ali pri ponudniku storitve.

5. Uporaba v avtomatiziranem nadzoru infrastructure

- Večina nadzornih sistemov (npr. Zabbix, PRTG, Nagios) uporablja ICMP kot osnovni mehanizem za preverjanje živosti naprav (angl. *host alive check*).
- V logističnih centrih to pomeni stalno spremljanje tisoč naprav – če ICMP ping ne uspe, sistem sproži opozorilo ali avtomatski restart.

8.8 Zakaj je to pomembno v praksi?

V praksi ICMP predstavlja **prvo linijo zaznavanja težav** v logističnih omrežjih.
Če povezava med terminalom in strežnikom WMS ne deluje, je ping najhitrejši način za preverjanje, kje v verigi je prekinitev.

Napake v omrežju se tako odkrijejo prej, preden povzročijo motnje v procesih, kot so:

- zastoj pri odpremi,
- nedelovanje čitalnikov kod ali tiskalnikov etiket,
- prekinitve v sinhronizaciji podatkov med lokacijami,
- neodzivnost transportnih API-jev ali oblačnih storitev.

8.9 Priporočila za logistična okolja

- Vzpostavi **redno ICMP spremljanje** (angl. ***ping monitoring***) za vse kritične sisteme (WMS, ERP, TMS, gateway, DNS).
- Implementiraj **avtomatske health-checke**, ki preverjajo dosegljivost in latenco.
- Vzdržuj **referenčne odzivne čase** (angl. **baseline**) za vsako lokacijo, saj to pomaga pri zaznavi degradacije povezav.
- Uporabi **traceroute** za analizo WAN poti in ugotavljanje, kje prihaja do zakasnitev.
- Omeji ICMP na notranje naslove ali dovoljena okolja — prepreči, da bi bil uporabljen za rekonstrukcijo topologije.
- Uporabi SIEM ali NMS za **samodejno beleženje in alarmiranje** ob izgubi ICMP odziva.
- Filtriraj samo nevarne tipe ICMP (npr. Echo Requests iz zunanjih virov), ne pa vseh. ICMP je ključen za pravilno delovanje IPv6 in MTU odkrivanje.

8.10 Varnostni vidik

- Napadalci ICMP uporabljajo za odkrivanje aktivnih sistemov (angl. *ping sweep*).
- Mogoč je ICMP tunneling – prenos podatkov mimo požarnih zidov.
- Traceroute razkriva omrežno topologijo, kar je uporabno tudi za napadalce.
- Prekomerno blokiranje ICMP (zlasti Packet Too Big in Time Exceeded) lahko zlomi IPv6 ali VPN delovanje. ICMP se uporablja tudi za exfiltracijo podatkov v naprednih napadih (ICMP tunneling).

– Pravilna politika: dovoliti osnovni ICMP za diagnostiko in MTU, a nadzorovati nenavadne vzorce prometa (npr. prekomerne pinge ali nenavadno dolge pakete).

ICMP je v logističnih omrežjih osnovni diagnostični mehanizem — "srčni utrip" omrežne povezljivosti.

Omogoča hitro preverjanje delovanja naprav, sistemov in povezav ter bistveno prispeva k **operativni stabilnosti, varnosti in učinkovitosti** celotne logistične infrastrukture.

8.11 Povzetek postopka preverjanja ICMP

Tabel 14

Korak	Ukaz	Namen
1	ping <gateway>	Preveri lokalno povezavo
2	ping <domena>	Preveri DNS + zunanjo povezavo
3	tracert / traceroute	Analiza poti do cilja
4	Dodatne možnosti	Napredna diagnostika
5	Interpretacija rezultatov	Odkrivanje napak in groženj

8.12 Tipične vaje / praktični koraki

1. ping <gateway> – preveri lokalno povezavo.
2. ping <domena> – preveri DNS in zunanjo povezavo.
3. tracert <domena> ali traceroute <domena> – prikaži pot do cilja in analizo zakasnitev.
4. ping -n 10 <IP> (Windows) ali ping -c 10 <IP> (Linux/macOS) – izvedi serijo testov in analizo izgub.
5. ping -l 1000 <domena> ali ping -s 1000 <domena> – preveri MTU in stabilnost povezave.
6. Analiziraj odzive: čas, TTL, izgube, neodzive.
7. Predlagaj ukrepe, če so odzivi nepričakovano dolgi ali paketov ni.

Univerzitetna založba
Univerze v Mariboru

9 Port number – številke vrat

9.1 Kaj je port number?

Angl. ***port number*** (številka vrat) je logični identifikator, ki pove, **kateri program ali storitev** na računalniku naj prejme podatke, poslane prek omrežja (Reynolds, 1992).

Medtem ko **IP naslov** določa, *na kateri računalnik* potuje promet, **port** določa, *kateri proces ali aplikacija* ga bo obdelala.

Vsaka naprava lahko istočasno izvaja več omrežnih storitev (npr. spletni strežnik, poštni strežnik, FTP, DNS …).

Zato je bil uveden sistem vrat, ki omogoča ločevanje teh storitev znotraj enega IP naslova.

Primer:

- IP: 192.168.1.10
- Port: 80
  → brskalnik se poveže na spletni strežnik (HTTP) te naprave.

9.2 Kako delujejo vrata?

Komunikacija med odjemalcem in strežnikom poteka prek dveh ključnih identifikatorjev:

- **IP naslov** – določa napravo v omrežju in
- **port številka** – določa aplikacijo/storitev na tej napravi.

Tako se ustvari angl. ***socket*** (vtič), ki ga določa kombinacija:

IP naslov + port = komunikacijska točka

Primer:

192.168.1.20:443

pomeni, da se povezujemo na napravo 192.168.1.20, vrata 443 (HTTPS).

9.3 Vrste vrat

Tabela 15

Obseg	Vrsta	Opis	Primer
0–1023	Well-known ports (standardna vrata)	Dodeljena najbolj znanim storitvam	80 (HTTP), 443 (HTTPS), 53 (DNS)
1024–49151	Registered ports (registrirana vrata)	Dodeljena določenim aplikacijam	3306 (MySQL), 8080 (alternativni HTTP)
49152–65535	Dynamic / Private ports (začasna ali zasebna)	Uporablja jih odjemalec pri vzpostavitvi povezav	dinamična izbira npr. 52481

9.4 Najpogosteje uporabljena vrata

Tabela 16

Storitev	Protokol	Vrata	Opis
HTTP	TCP	80	Prenos spletnih strani
HTTPS	TCP	443	Varni spletni prenos (TLS/SSL)
FTP	TCP	21	Prenos datotek
SSH	TCP	22	Varna oddaljena prijava
Telnet	TCP	23	Oddaljeni dostop (nevaren)
SMTP	TCP	25	Pošiljanje e-pošte
POP3	TCP	110	Prejemanje e-pošte
IMAP	TCP	143	Dostop do e-pošte
DNS	UDP/TCP	53	Pretvorba imen v IP naslove
DHCP	UDP	67, 68	Dodeljevanje IP naslovov
RDP	TCP	3389	Oddaljeni namizni dostop
SMB	TCP	445	Deljenje datotek v Windows
NTP	UDP	123	Sinhronizacija časa

9.5 TCP in UDP vrata

- **TCP vrata** zagotavljajo zanesljivo, potrjeno dostavo (npr. HTTP, HTTPS, SMTP).
- **UDP vrata** omogočajo hitrejšo, a manj zanesljivo komunikacijo (npr. DNS, DHCP, NTP).

Primer:

- DNS uporablja UDP/53 za hitre poizvedbe, vendar TCP/53 za prenos večjih odgovorov.
- HTTP deluje na TCP/80, ker potrebuje potrjevanje prenosa.

- **Kako preverimo odprta vrata?**

Windows:

```
netstat -an
```

Linux / macOS:

```
sudo netstat -tuln
```

ali

```
ss -tuln
```

Pomen oznak:

- t – TCP
- u – UDP
- l – listening (vrata, ki čakajo na povezavo)
- n – prikaži številke, ne imena

Primer: kaj se zgodi pri HTTP povezavi?

1. Brskalnik pošlje zahtevo na IP naslov strežnika prek **TCP vrat 80**.
2. Strežnik posluša na teh vratih in sprejme povezavo.
3. Ko strežnik odgovori, se vzpostavi dvosmerna komunikacija prek istih vrat.
4. Po koncu seje se vrata na strani odjemalca zaprejo.

9.6 Pomen za logistiko

Port number (številka vrat) določa, katera aplikacija ali storitev na računalniku sprejema ali pošilja podatke.

Vsak paket v protokolih **TCP** ali **UDP** ima poleg IP naslova tudi **številko vrat**, kar omogoča pravilno usmerjanje podatkov do ustreznega procesa.

V logističnih informacijskih sistemih porti omogočajo:

- delovanje aplikacij, kot so **WMS, ERP, TMS, EDI, IoT** in API-ji,
- komunikacijo s **strežniki podatkovnih baz, poštnimi in spletnimi storitvami**,
- integracijo z zunanjimi partnerji (npr. prevozniki, dobavitelji, carinski sistemi),
- ločevanje prometa po funkcionalnosti in varnostni politiki.

Brez pravilne uporabe portov ne bi bilo mogoče vzpostaviti povezave med aplikacijskimi storitvami, kar bi ohromilo digitalne procese v logistiki.

9.7 Zakaj je to pomembno v praksi?

Vsaka komunikacija v logističnem omrežju poteka prek določenih portov — ti so osnova za varno in učinkovito izmenjavo podatkov med sistemi.
Nekateri primeri iz prakse:

- **Port 80/443 (HTTP/HTTPS)** — za spletne portale in API-je (npr. https://wms.logistics.si/api).
- **Port 21/22 (FTP/SFTP)** — prenos EDI datotek ali nalepk na tiskalniške strežnike.
- **Port 25/587 (SMTP)** — pošiljanje e-poštnih obvestil o odpremi ali dostavi.
- **Port 1433 (MSSQL) ali 3306 (MySQL)** — dostop do baz podatkov ERP ali WMS sistemov.
- **Port 53 (DNS)** — razreševanje imen za strežnike in aplikacije.

Če so vrata napačno zaprta, odprta ali napačno preusmerjena:

- aplikacije ne delujejo (npr. WMS ne dostopa do baze),
- API-ji ne komunicirajo z zunanjimi partnerji,
- podatki se pošiljajo prek nezaščitenih kanalov, kar povzroča zamude, napake in varnostna tveganja.

9.8 Priporočila za logistična okolja

- **Vzpostavi natančen seznam dovoljenih portov** za vsako aplikacijo in okolje (produkcijsko, testno, razvojno).
- **Uporabi NGFW ali UTM požarni zid**, ki omogoča granularno kontrolo prometa po portih in aplikacijah.
- **Blokiraj vse neuporabljene porte** — naj bodo privzeto zaprti (princip "deny all, allow specific").
- **Uporabi ločene VLAN-e** in pravila, da se promet med logističnimi podsistemi izvaja samo prek dovoljenih portov.
- **Omogoči šifriranje komunikacije** na portih, kjer se prenašajo občutljivi podatki (npr. HTTPS, FTPS, SMTPS).
- **Spremljaj promet na neobičajnih portih**, saj se ti pogosto uporabljajo za napade ali prikrite kanale (npr. malware, tuneliranje).
- **Redno preverjaj konfiguracijo** NAT in port forwarding pravil, da preprečiš nenamerno izpostavitev notranjih strežnikov.
- **Vzpostavi centraliziran nadzor** (SIEM ali NMS), ki beleži dostop po portih in zazna anomalije.

9.9 Varnostni vidiki

Porti so najpogosteje uporabljena vstopna točka za kibernetske napade.

Najpogostejše grožnje vključujejo:

- **port scanning** — napadalci iščejo odprta vrata (npr. z nmap) za identifikacijo storitev
- **brute-force napade** na porte 22 (SSH), 3389 (RDP), 445 (SMB),
- **nezavarovane porte** (npr. 21 FTP brez TLS), ki omogočajo prestrezanje gesel in podatkov,
- **skrite tunele** (npr. HTTP ali DNS tuneliranje) za iznos podatkov prek dovoljenih portov,
- **RDP zlorabe** in **SMB ranljivosti** (WannaCry, EternalBlue).

Za zaščito:

- uporabi **firewall pravila** z "least privilege" pristopom,

- redno izvajaj **skeniranje odprtih portov** (npr. nmap, netstat -ano),
- uporabljaj **VPN** ali **Zero Trust** za oddaljene povezave,
- beleži vse **odprte TCP/UDP seje** v SIEM sistem,
- spremljaj in blokiraj poskuse **port scanov** ali **nenavadnih povezav**.

9.10 Tipične vaje / praktični koraki

1. Prikaz odprtih portov v sistemu:

- Windows: netstat -ano
- Linux/macOS: ss –tuln
- Zapiši, kateri porti so odprti in katera aplikacija jih uporablja.

2. Skeniranje oddaljenega sistema:

nmap 192.168.1.10
Identificiraj odprta vrata in preveri, ali ustrezajo pričakovanim storitvam.

3. Preveri port določene aplikacije:

netstat -b | find "wms.exe"
Ugotovi, na katerem portu aplikacija posluša.

4. Analiza v Wiresharku:

Filtriraj promet po portu:
tcp.port == 443
Opazuj HTTPS komunikacijo in preveri, ali gre za šifriran promet.

5. Simulacija napake:

Zapri port 1433 v požarnem zidu in preveri, ali se ERP še poveže z bazo.

6. Varnostna vaja:

Preveri, kateri porti so izpostavljeni iz zunanjega omrežja (npr. z shodan.io) in predlagaj, katere bi moral sistem zapreti.

7. Dopolnilna naloga:

Pripravi tabelo najpogostejših portov (HTTP, HTTPS, FTP, SMTP, DNS, SSH, RDP, SMB) z opisom in vlogo v logistiki.

Vaja 1 – Prepoznaj storitev

Dopolni tabelo:

Port	Protokol	Storitev	Opis
21	TCP		
53	UDP		
80	TCP		
443	TCP		
25	TCP		

Vaja 2 – Preveri odprta vrata

Odpri **ukazno vrstico** in izvedi:

```
netstat -an
```

Nato odgovori:

1. Katera vrata na tvojem računalniku so odprta (LISTENING)?
2. Katera vrata uporabljajo aplikacije za splet (npr. brskalnik)?
3. Katere storitve so dostopne od zunaj?

Vaja 3 – Praktični test v Wiresharku

1. Začni zajem prometa.
2. Odpri brskalnik in obišči https://www.um.si.
3. V Wiresharku uporabi filter:

```
tcp.port == 443
```

4. Opazuj paket, v katerem je tvoj računalnik *odjemalec* in strežnik *na vratih 443*.

5. Določi, katera vrata uporablja tvoj odjemalec (običajno naključna iz območja 49152–65535).

9.11 Povzetek

Tabela 17

Pojem	Pomen
Port number	Logični identifikator za posamezno storitev ali aplikacijo
Well-known ports	Vrata 0–1023, rezervirana za standardne protokole
Registered ports	Vrata 1024–49151, registrirana za specifične aplikacije
Dynamic ports	Začasna vrata, ki jih uporablja odjemalec
TCP vrata	Zanesljiva povezava (ACK, retransmisija)
UDP vrata	Hitrejša, brez potrjevanja
netstat / ss	Orodji za pregled odprtih vrat

Univerzitetna založba
Univerze v Mariboru

10 NAT – Network Address Translation

10.1 Kaj je NAT

NAT (angl. ***Network Address Translation***) je mehanizem, ki omogoča, da več naprav v **zasebnem omrežju** dostopa do interneta z **enim samim javnim IP naslovom** (Srisuresh in Holdrege, 1999).

Deluje kot **prevajalec naslovov**, ki med notranjimi (zasebnimi) in zunanjimi (javnim) omrežji pretvarja IP naslove in številke vrat.

NAT je danes nepogrešljiv v domačih in poslovnih omrežjih, saj:

- omogoča varnost (zunanjim uporabnikom skrije notranje naslove),
- zmanjšuje porabo javnih IP naslovov,
- omogoča hkratni dostop več notranjih naprav do interneta.

10.2 Zakaj potrebujemo NAT

IPv4 naslovni prostor je omejen (≈ 4,3 milijarde naslovov).

Ker bi bilo nemogoče, da bi vsak računalnik v svetu imel svoj javni IP, so bila uvedena **zasebna omrežja (RFC 1918)** in NAT.

NAT tako omogoča, da:

- znotraj podjetja ali doma uporabljamo zasebne naslove (npr. 192.168.x.x),
- usmerjevalnik (router) poskrbi, da promet pravilno "prevede" navzven in nazaj.

10.3 Kako NAT deluje

Ko notranja naprava pošlje podatke v internet, usmerjevalnik izvede:

1. **zamenjavo izvornega IP naslova** (npr. iz 192.168.1.10 v 84.255.12.90),
2. **shrani zapis v NAT tabelo**, da ve, komu naj pošlje odgovor,
3. **posreduje promet v internet** pod svojim javnim naslovom,
4. ko odgovor pride nazaj, **prevede cilj** in ga pošlje pravilni notranji napravi.

Primer

Tabela 18

Korak	Izvorni naslov	Ciljni naslov	Opis
1	192.168.1.10:50500	93.184.216.34:80	Uporabnik pošlje zahtevo (HTTP)
2	84.255.12.90:62001	93.184.216.34:80	Usmerjevalnik zamenja IP in vrata
3	93.184.216.34:80	84.255.12.90:62001	Strežnik odgovori
4	93.184.216.34:80	192.168.1.10:50500	NAT vrne odgovor notranjemu odjemalcu

10.4 Vrste NAT

Tabela 19

Vrsta NAT	Opis	Uporaba
Static NAT (1:1)	Vsaka notranja naprava ima stalno preslikavo v en javni IP.	Strežniki, kjer mora biti povezava dostopna od zunaj.
Dynamic NAT (n:1 ali n:m)	Notranje naprave uporabljajo poljubne javne naslove iz določenega nabora.	Večje organizacije z več zunanjimi naslovi.
PAT (Port Address Translation)	Več notranjih naprav si deli en javni naslov, ločevanje po številkah vrat.	Najpogostejši primer v domačih omrežjih.

10.5 PAT

Angl. *Port Address Translation* **(PAT)** je posebna oblika NAT, kjer se poleg IP naslova pretvarjajo tudi **številke vrat**.
Vsaka povezava dobi **unikatno kombinacijo** javnega IP + porta, da se ne zamenja z drugimi.

Primer:

Tabela 20

Notranji IP	Notranja vrata	Javni IP	Javni port
192.168.1.10	50000	84.255.12.90	61001
192.168.1.11	50000	84.255.12.90	61002
192.168.1.12	50000	84.255.12.90	61003

Tako lahko sto notranjih računalnikov uporablja isto zunanjo povezavo.

NAT tabela

NAT usmerjevalnik si zapomni aktivne preslikave v **NAT tabeli**.

Tabela 21

Notranji naslov	Notranja vrata	Zunanji naslov	Zunanja vrata	Status
192.168.1.10	50000	93.184.216.34	80	Active
192.168.1.11	50001	142.250.74.206	443	Active

Ko se povezava zaključi ali izteče čas (timeout), se vnos izbriše.

10.6 Prednosti NAT

- prihranek javnih IP naslovov,
- dodatna plast varnosti – notranji naslovi so skriti,
- enostavno upravljanje in nadzor prometa,
- združljivo z IPv4 standardom.

10.7 Slabosti NAT

- lahko otežuje dohodne povezave (npr. spletne kamere, igre, VoIP),
- povečuje kompleksnost pri konfiguraciji VPN,
- prekinja “end-to-end” načelo interneta.

10.8 Preveri NAT v praksi

Windows:

`ipconfig`
– preveri svoj lokalni IP naslov.

`tracert www.google.com`
– opazi, da prvi skok vodi na lokalni gateway (zasebni IP), končni pa na javni strežnik.

`nslookup myip.opendns.com resolver1.opendns.com`
– prikaže tvoj **javni IP naslov**, prek katerega gre ves promet.

Linux/macOS:

`ip addr show`
– lokalni IP.

`curl ifconfig.me`
– zunanji (javni) IP, ki ga dodeli NAT naprava.

Pomembni elementi

- **Inside Local Address** – notranji zasebni IP (npr. 192.168.0.10)
- **Inside Global Address** – javni IP po pretvorbi (npr. 93.103.44.10)
- **Outside Local Address** – IP zunanje naprave, kot ga vidi notranje omrežje
- **Outside Global Address** – dejanski IP zunanje naprave v internetu

10.9 Pomen za logistiko — NAT

V logističnih omrežjih NAT predstavlja **osnovni varnostni in funkcionalni sloj**, ki povezuje notranje informacijske sisteme (WMS, ERP, TMS, IoT senzorje) z zunanjimi dobavitelji, prevozniki in oblačnimi storitvami.

1. Omogoča povezljivost notranjih sistemov z zunanjim svetom

- Terminali, čitalniki, RFID bralniki in nadzorni sistemi dostopajo do strežnikov prek enega javnega IP.
- Omogoča centraliziran dostop brez potrebe po individualnih zunanjih IP-jih.

2. Varnost in izolacija notranjega omrežja

- Zunanje naprave ne morejo neposredno dostopati do notranjih IP-jev.
- NAT deluje kot dodatna plast obrambe skupaj z NGFW.

3. Podpora hibridnim in oblačnim okoljem

- Povezava med lokalnim WMS/ERP in SaaS aplikacijami (npr. SAP, Microsoft 365, logistični API-ji).
- NAT omogoča hkratne povezave več sto odjemalcev brez konflikta naslovov.

4. Optimizacija uporabe naslovnega prostora

- Zasebni IP naslovi zmanjšajo porabo javnih IPv4 naslovov.
- NAT omogoča migracijo na IPv6 z uporabo Dual Stack ali NAT64.

5. Integracija s SCADA, IoT in telemetrijo

- Senzorji v skladiščih, transportnih vozilih in hladilnih sistemih komunicirajo prek NAT-a do centralnih platform.

10.10 Zakaj je to pomembno v praksi

NAT je temelj delovanja sodobnih logističnih omrežij.

Omogoča varno, skalabilno in ekonomično povezljivost vseh komponent z internetom in zunanjimi partnerji.

V primeru napak pri NAT konfiguraciji pride do:

- nedelovanja WMS terminalov ali IoT naprav,
- onemogočenega dostopa do oblačnih storitev,
- neuspešne sinhronizacije podatkov med lokacijami,

kar lahko povzroči zastoje v transportu, komisioniranju ali sledenju pošiljk.

10.11 Priporočila za logistična okolja

- Uporabljaj **PAT** (NAT overload) za notranje uporabnike in IoT naprave.
- Za zunanje storitve (npr. dostop do WMS portala) uporabi **Static NAT** z NGFW.

- Redno preverjaj NAT tabele in trajanje sej, saj to prepreči prepolnitev NAT cache-a.
- Spremljaj povezave z **NetFlow/NTA**, da zaznaš nenavadne izhode (možni tuneli).
- Uporabi SIEM za beleženje NAT preslikav ob incidentih.
- Pri IPv6 uporabi **NPTv6 (Network Prefix Translation)** ali Dual Stack, ne klasičnega NAT.

10.12 Varnostni vidik

- **ICMP ali TCP tunneling skozi NAT** – napadalci lahko uporabijo NAT za prikrivanje povezav.
- **NAT slipstreaming** – metoda za obvoz požarnega zidu in dostop do notranjih storitev.
- **Nepravilno nastavljen Static NAT** lahko razkrije notranje strežnike.
- **NAT logi** so bistveni za forenzične analize (povezava med notranjim IP in javnim IP/portom).
- **Pravilna konfiguracija NGFW + NAT** zagotavlja sledljivost in preprečuje nepooblaščen promet.

10.13 Tipične vaje / praktični koraki

1. Preveri svoj lokalni IP (ipconfig / ip addr).
2. Uporabi curl ifconfig.me ali obišči https://whatismyip.com za javni IP.
3. Primerjaj oba naslova – razlika pomeni delovanje NAT.
4. Na usmerjevalniku (če imaš dostop) prikaži NAT tabelo in poišči svoj notranji IP.
5. Izvedi tracert www.google.com – opazuj prvi zasebni in zadnji javni skok.
6. Analiziraj, kako NAT vpliva na dostop do zunanjih strežnikov.
7. Pripravi shemo omrežja z označenimi notranjimi in javnimi naslovi.

Po potrebi razloži, kako bi konfiguriral Static NAT za WMS strežnik.

Vaja 1 – Analiza NAT tabele

Predstavljaj si, da tvoj računalnik z naslovom 192.168.0.5 odpira spletno stran.

Dopolni tabelo:

Notranji IP	Notranja vrata	Javni IP	Javni port	Cilj IP	Ciljna vrata

Vaja 2 – Opazuj NAT v praksi

1. Odpri ukazno vrstico in vpiši:

```
nslookup www.google.com
```

2. V Wiresharku uporabi filter:

```
ip.src == tvoj_notranji_IP || ip.dst == tvoj_javni_IP
```

3. Opazuj, kako se pri izhodnih paketih IP naslovi in vrata razlikujejo od povratnih.

Vaja 2 – Opazuj NAT v praksi

1. Odpri brskalnik na dveh napravah v istem omrežju.
2. Obišči stran **https://whatismyip.com**.
3. Kljub različnim notranjim IP-jem (npr. 192.168.1.5 in 192.168.1.6) bosta obe napravi prikazali **isti javni IP** – tistega od tvojega usmerjevalnika. To je rezultat NAT pretvorbe.

10.14 Povzetek postopka preverjanja NAT

Tabela 22

Korak	Ukaz	Namen
1	ipconfig / ip addr	Preveri notranji IP naslov
2	nslookup / curl ifconfig.me	Preveri javni IP (preko NAT)
3	tracert / traceroute	Analiza poti do cilja
4	Preveri NAT tabelo v usmerjevalniku	Preveri aktivne preslikave
5	Analiza logov	Povezava notranjih IP-jev z zunanjimi sejami

Univerzitetna založba
Univerze v Mariboru

11 ARP

11.1 Kaj je ARP

ARP (angl. ***Address Resolution Protocol***) je protokol, ki v lokalnem omrežju (LAN) **pretvarja IP naslove v fizične MAC naslove**.

Deluje na **povezovalni plasti (Layer 2)** in omogoča, da se podatkovni paketi z naslovi IP pravilno dostavijo napravam, ki komunicirajo prek omrežnih kartic (Ethernet).

Čeprav IP določa *logični naslov naprave*, mora za dejanski prenos po lokalnem omrežju računalnik poznati **MAC naslov** naprave, s katero komunicira. ARP poskrbi za to povezavo.

11.2 Zakaj potrebujemo ARP

Vsaka naprava v omrežju ima:

- **IP naslov** (npr. 192.168.1.10) – logični naslov za identifikacijo v omrežju,
- **MAC naslov** (npr. 00-1A-2B-3C-4D-5E) – fizični naslov omrežne kartice.

Ko računalnik želi poslati paket na določen IP naslov v istem omrežju, najprej preveri, ali pozna ustrezen MAC naslov:

- če ga **že pozna**, uporabi podatek iz **ARP predpomnilnika (cache)**,
- če ga **ne pozna**, pošlje **ARP zahtevo (ARP Request)** vsem napravam v omrežju (broadcast).

11.3 Kako deluje ARP

1. Računalnik pošlje *ARP Request* sporočilo:
   »Kdo ima IP naslov 192.168.1.20?«
   To sporočilo prejmejo vse naprave v lokalnem omrežju.
2. Naprava, ki ima ta IP, odgovori z *ARP Reply*:
   »IP 192.168.1.20 pripada MAC naslovu 00-1A-2B-3C-4D-5E.«
3. Pošiljatelj si to povezavo shrani v **ARP cache**, da pri naslednji komunikaciji ne pošilja nove zahteve.

Primer komunikacije

Tabela 23

Korak	Vrsta sporočila	Vsebina	Opis
1	ARP Request	Kdo ima IP 192.168.1.20?	Računalnik A sprašuje po MAC naslovu
2	ARP Reply	IP 192.168.1.20 je pri 00-1A-2B-3C-4D-5E	Računalnik B odgovori
3	Vnos v ARP cache	192.168.1.20 → 00-1A-2B-3C-4D-5E	Računalnik A shrani preslikavo

11.4 Preverjanje ARP

Odpri ukazno vrstico / terminal

Windows

– Pritisni **Win + R** → vpiši cmd → Enter

Linux / macOS

– Odpri **Terminal**

Prikaži trenutno ARP tabelo

Windows:

```
arp -a
```

Linux / macOS:

```
arp -n
```

Rezultat je seznam IP naslovov in njihovih pripadajočih MAC naslovov, ki jih je sistem zaznal v zadnjem času.

Primer (Windows):

```
Interface: 192.168.0.15 --- 0x7
  Internet Address      Physical Address      Type
  192.168.0.1           aa-bb-cc-dd-ee-ff     dynamic
  192.168.0.23          00-15-5d-00-12-34     dynamic
```

Primer (Linux):

```
Address         HWtype  HWaddress           Flags Mask            Iface
192.168.0.1     ether   aa:bb:cc:dd:ee:ff   C                     wlan0
192.168.0.23    ether   00:15:5d:00:12:34   C                     wlan0
```

Osveži ARP tabelo (če je prazna)

Če je tabela prazna, moraš najprej generirati omrežni promet do lokalnih IP naslovov, da se ARP vnosi pojavijo.

Najlažji način:

```
ping 192.168.0.1
```

ali

```
ping 192.168.0.255   # broadcast ping
```
(Windows ne podpira vedno)

Nato ponovno poglej ARP tabelo:

```
arp -a
```

Preveri MAC naslov privzetega prehoda (gateway)

Privzeti prehod je običajno **prvi IP v omrežju** (npr. 192.168.0.1).

Ta zapis je pomemben, ker ARP uporablja terminal za izhod iz lokalnega omrežja.

Preveri svoj gateway z ukazom:

```
ipconfig
```
(poglej vrstico "Default Gateway")

Nato v ARP tabeli poišči **MAC naslov za ta IP**.

Če se MAC naslov spremeni nenavadno pogosto ali je "neznan", lahko gre za ARP spoofing.

Preveri sumljive vnose

Pazi na:

- **Isti MAC naslov za več IP naslovov** → lahko znak zlorabe (man-in-the-middle).
- **MAC naslov gatewaya, ki se ne ujema s pričakovanim** → preveri pri administratorju.
- **Stari ali statični vnosi** → lahko povzročajo težave pri komunikaciji.

Za primerjavo lahko uporabiš:

- navodila ponudnika usmerjevalnika (MAC naslov naprave),
- ip neigh show (Linux) za dodatne informacije.

11.5 Pomen za logistiko

ARP (angl. *Address Resolution Protocol*) je **osnovni mehanizem povezovanja IP in MAC naslovov** v lokalnem omrežju. Omogoča, da se IP paketi pravilno prevedejo na fizične naslove naprav, kar je pogoj za delovanje vseh notranjih logističnih sistemov, od skladiščnih terminalov do podatkovnih strežnikov.

V logističnih omrežjih, kjer delujejo stotine ali tisoči povezanih naprav (terminali, tiskalniki, RFID čitalniki, PLC krmilniki), pravilno delovanje ARP zagotavlja **zanesljivost, odzivnost in varnost komunikacije** v realnem času.

1. Zanesljivo delovanje lokalnih omrežij

- ARP omogoča hitro pretvorbo IP naslovov v MAC naslove, kar je ključno za delovanje LAN komunikacije med logističnimi napravami.
- Brez pravilno delujočega ARP protokola ne bi bilo mogoče komunicirati znotraj istega omrežnega segmenta (npr. med WMS strežnikom in ročnim terminalom).
- V logističnih skladiščih, kjer se podatki posodabljajo v realnem času, ARP omogoča neprekinjen prenos informacij o zalogah, statusih in lokacijah.

2. Avtomatsko odkrivanje in integracija naprav

- Logistična omrežja so dinamična – terminali, vozila in senzorji se pogosto priklapljajo in odklapljajo.
- ARP omogoča, da se nove naprave **samodejno prepoznajo** in povežejo brez ročnega vnosa MAC naslovov.
- Tako se pospeši inicializacija novih komponent (npr. RFID bralnikov ali avtomatskih tehtnic) in zmanjša možnost napak pri konfiguraciji.

3. Podpora za operativno učinkovitost in redundanco

- ARP tabele zagotavljajo, da se promet usmerja prek najbližjih ali aktivnih vmesnikov, kar optimizira odzivnost aplikacij (ERP, WMS, TMS).
- V redundantnih omrežjih (npr. dvojni prehodi) omogoča pravilno preklapljanje poti, ko ena naprava odpove.
- To zmanjšuje izpade komunikacije in povečuje zanesljivost delovanja transportnih procesov.

4. Zaznavanje napak in anomalij v omrežju

- Z ukazom arp -a (Windows) ali arp -n (Linux) lahko administrator preveri, ali se IP naslovi pravilno ujemajo z MAC naslovi.
- Nenavadne spremembe (isti MAC za več IP-jev, neznani naslovi) so lahko znak **tehničnih napak ali kibernetskih napadov**.
- V logističnih okoljih, kjer se podatkovni tokovi nenehno usmerjajo med podsistemi, je nadzor ARP tabel ključnega pomena za zagotavljanje integritete komunikacij.

5. Varnostni in forenzični pomen

- ARP sam po sebi ne vključuje avtentikacije, saj vsak sistem v omrežju lahko pošlje lažen ARP odgovor.
- Tako so možni napadi, kot sta **ARP spoofing** ali **man-in-the-middle (MITM)**, kjer napadalec preusmeri promet prek svoje naprave.
- V logističnem kontekstu to pomeni potencialno prestrezanje poslovno občutljivih podatkov: naročil, transportnih poti ali zalog.
- Spremljanje ARP vedenja je pomemben del **incident response** postopkov in **forenzične analize** notranjih napadov.

11.6 Zakaj je to pomembno v praksi

Napake ali zlorabe v ARP tabelah so med najpogostejšimi vzroki za motnje v lokalnih omrežjih.

Pogoste težave vključujejo:

- dvojne IP naslove ali napačno konfigurirane vmesnike,
- napačne ali statične ARP vnose, ki povzročajo "blackhole" promet,
- spoofane MAC naslove, ki preusmerjajo promet napadalcu,
- nepravilno delovanje redundančnih povezav zaradi napačnih ARP mapiranj.

V logističnih omrežjih to lahko vodi do:

- prekinitev komunikacije med terminali in WMS,
- zamud pri prenosu podatkov o pošiljkah,
- napačnih statusov zalog zaradi izgubljenih paketov,
- popolne zaustavitve avtomatiziranih procesov (npr. roboti, tekoči trakovi).

11.7 Priporočila za logistična okolja

- Redno preverjaj ARP tabele in spremljaj spremembe MAC naslovov ključnih naprav (gateway, strežniki).
- Uporabi orodja za **detekcijo ARP spoofinga** (npr. Arpwatch, XArp, Wireshark filtri).
- Na stikalih omogoči **Dynamic ARP Inspection (DAI)** in **port security**, da preprečiš lažne ARP odgovore.

- Vzpostavi ARP **statiko** za kritične naprave (npr. prehode, WMS strežnike).
- Vključi ARP nadzor v **SIEM** sistem, da se anomalije zaznajo samodejno.
- Uporabi **segmentacijo omrežja (VLAN)** za zmanjšanje možnosti MITM napadov.
- Uči uporabnike prepoznavati znake napadov, kot so prekinitve povezav ali nenavadne počasnosti sistema.

ARP je **temeljni gradnik zanesljive lokalne komunikacije** v logističnih in industrijskih omrežjih.

Omogoča učinkovito povezovanje med napravami, samodejno zaznavanje novih komponent in stabilno delovanje aplikacij v realnem času.

Hkrati pa predstavlja tudi **potencialno varnostno tveganje**, če ni ustrezno nadzorovan.

Njegovo pravilno razumevanje in redno preverjanje sta bistvena za **operativno kontinuiteto in varnost logističnih informacijskih sistemov**.

11.8 Varnostni vidik

- ARP je **nezavarovan protokol** — vsak v istem omrežju lahko pošilja lažne ARP odgovore (»ARP spoofing«).
- Zato je poznavanje ARP tabel uporabno za **preverjanje legitimnosti lokalnih komunikacij** (npr. pri Kill Chain analizi, Recon fazi ali incidentih).

11.9 Tipične vaje / praktični koraki

1. Prikaži trenutno ARP tabelo (arp -a / arp -n) in zabeleži vnose.
2. Osveži tabelo z ukazom ping <IP> in ponovno preveri spremembe.
3. Identificiraj MAC naslov privzetega prehoda (ipconfig → “Default Gateway”).
4. Preveri, ali se MAC naslov gatewaya ujema z dejanskim naslovom naprave.
5. Zaznaj morebitne podvojene ali sumljive ARP vnose.
6. Preizkusi orodje za zaznavanje ARP spoofinga in analizo prometa.
7. Pripravi poročilo o vplivu napačnega ARP mapiranja na delovanje WMS ali ERP sistema.

11.10 Vaje

Vaja 1 – Preveri ARP tabelo

1. Odpri ukazno vrstico (cmd ali PowerShell).
2. Vpiši:
   arp -a
3. Zapiši vsaj dva zapisa iz tabele.
4. Določi:
   - kateri IP pripada tvojemu usmerjevalniku,
   - kateri napravi pripadajo drugi MAC naslovi.

Vaja 2 – Ponovni priklic ARP

1. Počisti ARP predpomnilnik:
   arp -d *
2. Ponovno obišči spletno stran (npr. https://fl.um.si).
3. Izvedi ukaz arp -a še enkrat in opazuj, kako se je tabela napolnila na novo.

Vaja 3 – Opazuj ARP promet v Wiresharku

1. Zaženi Wireshark in nastavi filter:
   arp
2. Pošlji ping znotraj svojega omrežja (npr. ping 192.168.1.1).
3. Opazuj:
   - ARP Request in ARP Reply pakete,
   - kdo jih pošilja in kdo odgovarja,
   - ali je odgovor shranjen v ARP tabeli.

11.11 Povzetek

Tabela 24

Korak	Ukaz	Namen
1	arp -a (Windows) / arp -n (Linux)	Pregled trenutnih ARP vnosov
2	ping <IP>	Osvežitev ARP tabel
3	ipconfig	Preverjanje privzetega prehoda
4	primerjava MAC naslovov	Odkrivanje anomalij ali ARP spoofinga

Univerzitetna založba
Univerze v Mariboru

12 MAC naslov

12.1 Kaj je MAC naslov

MAC naslov (angl. *Media Access Control address*) je **edinstveni fizični identifikator** omrežne kartice ali vmesnika.

Vsaka naprava, ki se povezuje v omrežje (računalnik, usmerjevalnik, tiskalnik, telefon …), ima svoj MAC naslov, ki jo loči od vseh drugih naprav na podatkovni plasti (Layer 2 – povezovalna plast).

MAC naslov je **vgrajen v strojno opremo** proizvajalca in se uporablja znotraj lokalnega omrežja (LAN), da se zagotovi pravilno usmerjanje okvirjev (frames).

12.2 Zgradba MAC naslova

MAC naslov je dolg **48 bitov (6 bajtov)** in je običajno zapisan v **16-tiškem (heksadecimalnem)** formatu.

Primeri zapisa:

```
00-1A-2B-3C-4D-5E
00:1A:2B:3C:4D:5E
001A.2B3C.4D5E
```

Prvih **24 bitov** predstavlja **identifikator proizvajalca** (angl. *OUI – Organizationally Unique Identifier*), zadnjih **24 bitov** pa **edinstveno številko naprave**, ki jo določi proizvajalec.

Tabela 25

Del	Ime	Pomen	Primer
00:1A:2B	OUI	Določa proizvajalca	00:1A:2B = Intel Corporation
3C:4D:5E	NIC ID	Določa posamezno napravo	Unikatno za vsak vmesnik

12.3 Vrste MAC naslovov

Vrsto MAC naslova določa že njegov zapis. Najnižji bit prvega bajta pove, ali je naslov individualen ali skupinski, zato ločimo tri vrste. Vsaka naprava ima svoj individualni (unicast) naslov, skupinski (multicast) in razpršeni (broadcast) naslov pa se uporabljata kot ciljna naslova, kadar je okvir namenjen več napravam hkrati.

Tabela 26

Vrsta	Opis	Primer uporabe
Unicast	Določa eno samo napravo	Komunikacija med dvema računalnikoma
Multicast	Paket se pošlje več napravam v skupini	Videokonference, pretakanje
Broadcast	Paket prejmejo vse naprave v lokalnem omrežju	ARP Request, DHCP Discover

12.4 Kako MAC sodeluje pri prenosu podatkov

Ko računalnik pošilja podatke v lokalno omrežje:

1. IP sloj določi cilj (npr. 192.168.1.10),
2. ARP protokol poišče ustrezen MAC naslov (npr. 00-1A-2B-3C-4D-5E),
3. ethernet okvir se pošlje na ta MAC naslov,
4. samo naprava z ustreznim MAC naslovom sprejme paket.

Tako se zagotovi, da v istem omrežnem segmentu ni napačnih dostav.

12.5 Prikaz MAC naslova v sistemu

Windows (PowerShell / cmd):

```
getmac
```

ali

```
ipconfig /all
```

Linux / macOS:

```
ip link show
```

ali

```
ifconfig
```

Primer (Windows):

```
Fizični naslov   . . . . . . . . . . : 00-1A-2B-3C-4D-5E
Opis . . . . . . . . . . . . . . . . : Intel(R) Ethernet Adapter
```

12.6 MAC naslov in varnost

MAC naslov se v praksi lahko **ponaredi (MAC spoofing)**, kar napadalcu omogoča, da se predstavi kot druga naprava.

To se pogosto uporablja pri testiranju ali pri dostopnih kontrolah, ki temeljijo samo na MAC filtriranju.

Primeri varnostnih ukrepov:

- filtriranje dovoljenih MAC naslovov na brezžičnem usmerjevalniku,
- preverjanje pristnosti z višjimi sloji (npr. 802.1X),
- zaznavanje sprememb MAC naslovov na omrežnih stikalih (port security).

12.7 Pomen za logistiko

MAC (Media Access Control) naslov je edinstvena fizična oznaka, dodeljena vsakemu omrežnemu vmesniku (npr. mrežni kartici, Wi-Fi modulu, tiskalniku, IoT napravi).

MAC naslov omogoča prepoznavanje in komunikacijo naprav na **podatkovni plasti (Layer 2)** omrežnega modela OSI.

V logističnih informacijskih sistemih ima MAC naslov pomembno vlogo pri:

- identifikaciji naprav (terminali, roboti, tiskalniki, kamere, senzorji),
- nadzoru dostopa do omrežja (Network Access Control, VLAN segmentacija),
- sledenju gibanja naprav v skladišču (Wi-Fi beacons, asset tracking),
- zagotavljanju varnosti in sledljivosti v notranjih omrežjih.

Ker je MAC naslov fizična identiteta naprave, predstavlja osnovo za povezljivost in nadzor nad omrežno infrastrukturo v logističnih okoljih.

12.8 Zakaj je to pomembno v praksi

Vsaka omrežna komunikacija v logističnem sistemu se začne z MAC naslovom – brez pravilnega delovanja ARP in MAC tabele ni povezave niti do bližnjega preklopnika (switcha).

V praksi to pomeni:

- če ima naprava napačno ali podvojeno MAC identiteto, se lahko komunikacija prekine,
- če je MAC naslov neznan, se naprava ne poveže v omrežje (blokada po varnostni politiki NAC),
- če pride do ARP spoofinga ali MAC floodinga, lahko napadalec preusmeri ali prestreže promet,
- da se pri sledenju sredstev v skladišču lahko MAC uporablja za identifikacijo mobilnih terminalov in IoT senzorjev.

Primer:

- Če AGV robot ne dobi IP naslova preko DHCP zaradi napačne MAC registracije, se ne bo prijavil v centralni sistem.
- Če se dva terminala prijavita z enakim MAC naslovom, bo omrežje povzročalo kolizije in izgubo povezav.
- Če je MAC filtriranje nepravilno nastavljeno, se lahko v notranje Wi-Fi omrežje poveže nepooblaščena naprava.

12.9 Priporočila za logistična okolja

- **Vzdržuj ažuren register MAC naslovov** za vse naprave v omrežju (npr. terminali, tiskalniki, IoT).
- **Uporabljaj 802.1X ali NAC (Network Access Control)** za preverjanje identitete naprav na podlagi MAC naslova.
- **Omogoči MAC-based VLAN segmentacijo**, da se naprave razvrščajo v ustrezna omrežja (uprava, skladišče, IoT).
- **Prepreči podvajanje MAC naslovov** – preverjaj jih v DHCP strežniku ali SIEM sistemu.
- **Uporabi statično dodeljene MAC-IP pare** za kritične naprave (npr. strežnike, tiskalnike, kontrolerje).
- **Redno spremljaj ARP in MAC tabele** na preklopnikih ter išči anomalije (nenavadne spremembe naslovov).
- **Uporabi ločene VLAN-e** za naprave z nizko varnostjo (npr. IoT, senzorje) in omeji njihovo komunikacijo na višje sloje.
- **Omogoči logiranje in korelacijo MAC dogodkov** v SIEM, kar olajša forenzično analizo in zaznavo zlorab.

12.10 Varnostni vidiki

MAC naslov je pogosto tarča manipulacij in zlorab, saj omogoča dostop do notranjega omrežja brez dodatne avtentikacije.

Najpogostejše grožnje:

- **MAC spoofing** — napadalec spremeni svoj MAC naslov, da se predstavi kot legitimna naprava.
- **MAC flooding** — preplavljanje preklopnika z lažnimi MAC naslovi, kar povzroči preusmeritev prometa (switch v "hub mode").
- **ARP spoofing / ARP poisoning** — povezano z MAC manipulacijami, omogoča prestrezanje prometa ali DoS napade.
- **Nezaščitena Wi-Fi omrežja** — napadalec pridobi MAC naslov naprave in posnema njeno identiteto (deauth attack).

Za zaščito:

- omogoči **port security** na stikalu (določi število in vrsto dovoljenih MAC naslovov),
- uporabi **802.1X avtentikacijo** in RADIUS strežnik,
- nadzoruj **neobičajne MAC spremembe** v ARP tabelah,
- filtriraj **sumljive MAC naslove** (npr. "00:00:00:00:00:00" ali "FF:FF:FF:FF:FF:FF"),
- spremljaj povezave z **neznanih proizvajalcev** (OUI – Organizationally Unique Identifier).

12.11 Tipične vaje / praktični koraki

1. Prikaži MAC naslov svoje naprave:

- Windows: ipconfig /all
- Linux/macOS: ip addr show

  Zapiši fizični naslov svoje mrežne kartice (npr. 00-1A-2B-3C-4D-5E).

2. Preveri MAC tabelo na stikalu ali routerju:

```
arp -a
```

Analiziraj, katere IP naslove in MAC naslove sistem pozna.

3. Z Wiresharkom zajemi lokalni promet in filtriraj po MAC naslovu:

```
eth.addr == 00:1A:2B:3C:4D:5E
```

Opazuj, kateri protokoli uporabljajo ta naslov.

4. Preveri proizvajalca naprave (OUI):

Obišči https://macvendors.com in vpiši MAC naslov – zapiši, kateremu proizvajalcu pripada.

5. Simuliraj napako:

Na dveh virtualnih napravah nastavi isti MAC naslov in preveri, kaj se zgodi z omrežno povezavo.

6. **Varnostni test:**
   Poskusi zaznati lažni MAC naslov z ukazom:
   arp -a | find "dynamic"

Primerjaj rezultate in razmisli, kako bi sistem zaščitil z uporabo port security.

7. **Analiza v praksi:**
   Pripravi seznam MAC naslovov naprav v skladišču in označi, katere so kritične za poslovanje (npr. RFID bralniki, WMS terminali).



Vaja 1 – Prepoznaj svoj MAC naslov

1. Odpri **ukazno vrstico (cmd)** in vpiši:
   getmac
2. Zapiši rezultat za aktivni omrežni vmesnik.
3. Določi proizvajalca glede na prvih 6 znakov (OUI).
   Poišči ga na spletni strani:
   https://macvendors.com



Vaja 2 – Poveži IP in MAC

1. Odpri **PowerShell** in vpiši:
   arp -a
2. V tabeli poišči MAC naslov svojega usmerjevalnika.
3. Primerjaj ga s podatki v ipconfig /all.
4. Pojasni, kako ARP uporablja MAC naslov za pošiljanje podatkov.



Vaja 3 – Opazuj MAC v Wiresharku

1. Zaženi Wireshark.
2. Nastavi filter:
   eth
3. Izvedi ping na drugo napravo v omrežju.
4. Opazuj polji **Source** in **Destination**, ki prikazujeta MAC naslova obeh naprav.

12.12 Povzetek

Tabela 27

Pojem	Pomen
MAC naslov	Edinstven fizični naslov omrežne kartice
OUI	Določa proizvajalca naprave
NIC ID	Določa posamezno napravo
Unicast / Broadcast / Multicast	Način dostave okvirjev v LAN-u
Ukaz getmac	Prikaže lokalni MAC naslov
MAC spoofing	Ponarejanje fizičnega naslova
Port security	Mehanizem za zaščito pred ponarejanjem MAC naslovov

Univerzitetna založba
Univerze v Mariboru

13 Ovijanje – pot podatkov skozi sloje omrežja

13.1 Kaj je enkapsulacija

Enkapsulacija (angl. ***encapsulation***) je proces, pri katerem se podatki med pošiljanjem **ovijajo** v zaporedne sloje dodatnih informacij (glave in repi paketov) (Woodburn in Mills, 1991).

Vsak sloj **dodaja svoje kontrolne podatke**, ki omogočajo prenos, usmerjanje in pravilno dostavo podatkov med napravami v omrežju.

Ko podatki potujejo nazaj (v nasprotni smeri, pri prejemniku), poteka obratni proces – **deenkapsulacija (decapsulation)**, kjer se dodatne informacije postopno odstranjujejo.

13.2 Zakaj je enkapsulacija pomembna

Omrežna komunikacija temelji na **modelu OSI** (angl. *Open Systems Interconnection*) ali **TCP/IP**.

Vsak sloj v modelu ima svojo vlogo, zato mora vsak dodati svoje podatke, da se prenos lahko izvede pravilno.

Enkapsulacija omogoča:

- združljivost med različnimi tehnologijami in napravami,
- zanesljivo dostavo podatkov,

– logično razmejitev nalog (aplikacija, omrežje, strojna oprema).

13.3 OSI model in enkapsulacija

Tabela 28

OSI sloj	Ime sloja	Enota podatka	Tipičen primer
7	Aplikacijski	Podatek (Data)	HTTP, FTP, DNS
6	Predstavitveni	Podatek	Kodiranje, šifriranje (TLS)
5	Sejni	Podatek	Upravljanje sej
4	Transportni	Segment	TCP, UDP
3	Omrežni	Paket	IP (IPv4, IPv6)
2	Povezovalni	Okvir (Frame)	Ethernet, Wi-Fi
1	Fizični	Bit	Električni ali optični signal

13.4 Kako poteka enkapsulacija

Ko pošiljamo npr. e-pošto ali obiskujemo spletno stran, podatki prehajajo skozi sloje od vrha navzdol:

1. **Aplikacijski sloj (HTTP, DNS, SMTP …)**
   → ustvari uporabniški podatek (npr. zahtevo za spletno stran).

2. **Transportni sloj (TCP ali UDP)**
   → doda **glavo** z informacijami o izvornih in ciljnih vratih.
   → podatkovna enota se imenuje **segment**.

3. **Omrežni sloj (IP)**
   → doda **IP glavo** z naslovoma pošiljatelja in prejemnika.
   → enota se imenuje **paket**.

4. **Povezovalni sloj (Ethernet / Wi-Fi)**
   → doda **MAC naslova** (izvorni in ciljni) ter preverjanje napak (CRC).
   → enota se imenuje **okvir (frame)**.

5. **Fizični sloj**
   → podatki se pretvorijo v **binarne signale** (0 in 1) in potujejo po kablu ali zraku.

Na ciljni strani poteka **deenkapsulacija** v obratnem vrstnem redu: fizični sloj → povezovalni → omrežni → transportni → aplikacijski.

Prikaz procesa

Pošiljanje podatkov (enkapsulacija)

```
Uporabnik → Brskalnik (HTTP)
      ↓
TCP → doda vrata
      ↓
IP → doda IP naslova
      ↓
Ethernet → doda MAC naslova
      ↓
Fizični sloj → 0 in 1 → omrežje
```

Prejemanje podatkov (deenkapsulacija)

```
Omrežje → Fizični sloj → Ethernet → IP → TCP → Aplikacija
```

13.5 Primer: obisk spletne strani

Ko vpišeš **https://www.um.si**, se zgodi naslednje:

1. brskalnik ustvari **HTTP(S) zahtevo**,
2. **DNS** pretvori ime www.um.si v IP naslov,
3. **TCP** vzpostavi povezavo s strežnikom na vratih 443,
4. **IP** določi, po kateri poti naj paket potuje,
5. **ethernet** doda fizične (MAC) naslove,
6. **NAT** na usmerjevalniku spremeni notranji naslov v javnega,
7. podatki potujejo po internetu in se pri cilju postopno **deenkapsulirajo**,
8. strežnik prebere HTTP zahtevo in pošlje odgovor, ki gre po isti poti nazaj.



Vaja 1 – Analiza slojev v Wiresharku

1. Zaženi **Wireshark** in v filter vpiši:

   ip.addr == tvoj_IP

2. Odpri brskalnik in obišči https://www.um.si.
3. Klikni en paket v Wiresharku in razširi posamezne sloje:

- Frame,
- Ethernet II,
- Internet Protocol (IP),
- Transmission Control Protocol (TCP),
- Hypertext Transfer Protocol (HTTP).

4. Opazuj, kako je vsak sloj dodal svoj del glave.

Vaja 2 – Razčleni paket

Dopolni tabelo s podatki iz Wiresharka:

Sloj	Protokol	Ključni podatki	Pomen
Povezovalni	Ethernet II	MAC izvorni / MAC ciljni	Fizična dostava
Omrežni	IP	IP naslova	Usmerjanje med omrežji
Transportni	TCP	Vrata 443 / 52341	Prenos sej
Aplikacijski	HTTPS	GET /index.html	Uporabniški podatek

Vaja 3 – Sestavi verigo enkapsulacije

Zapiši zaporedje protokolov, ki sodelujejo, ko pošlješ zahtevo:

URL → DNS → IP → TCP → Port → NAT → ARP → MAC → Enkapsulacija

Pojasni, kako vsak korak prispeva k uspešni dostavi podatkov.

13.6 Povzetek

Tabela 29

Pojem	Pomen
Enkapsulacija	Postopek ovijanja podatkov z glavo posameznega sloja
Deenkapsulacija	Obraten proces odstranjevanja glave ob sprejemu
OSI model	Referenčni okvir za razumevanje komunikacije
Slojni pristop	Omogoča modularnost in združljivost protokolov
Enota podatka	Frame, Packet, Segment, Data
Wireshark	Orodje za analizo enkapsulacije v praksi

Univerzitetna založba
Univerze v Mariboru

14 Celoten potek – Od URL do prikaza spletne strani

14.1 Uvod

Ko uporabnik vpiše spletni naslov (URL) v brskalnik, se v ozadju sproži zapleten niz omrežnih procesov, ki vključujejo prevajanje imen, vzpostavljanje povezav, usmerjanje, preverjanje naslovov in fizični prenos podatkov.

Vsak sloj omrežnega modela, od **aplikacijskega (HTTP, DNS)** do **fizičnega (Ethernet, Wi-Fi)**, ima pri tem svojo nalogo,

Razumevanje tega poteka je ključno za razumevanje delovanja interneta, odpravljanje težav in zagotavljanje varnosti v omrežjih.

14.2 Potek komunikacije – korak za korakom

Tabela 30

Korak	Proces	Opis	Uporabljeni protokoli
1	Vnos URL	Uporabnik vpiše npr. https://www.um.si. Brskalnik prepozna protokol (HTTPS) in domeno.	URL
2	Prevod domene	DNS strežnik pretvori ime www.um.si v IP naslov (npr. 164.8.100.110).	DNS
3	Ugotavljanje poti	Brskalnik pripravi TCP povezavo s ciljem na ustreznih vratih (443).	IP, TCP
4	Preverjanje vrat	Sistem uporabi port number, da ve, katera aplikacija bo prejela podatke.	TCP, UDP
5	Pretvorba naslovov	NAT na usmerjevalniku prevede notranji IP (192.168.x.x) v javnega (84.x.x.x).	NAT

Korak	Proces	Opis	Uporabljeni protokoli
6	Določitev MAC naslova	ARP pridobi fizični naslov naprave znotraj lokalnega omrežja.	ARP
7	Dodajanje okvirjev	Ethernet doda MAC naslova pošiljatelja in prejemnika.	Ethernet (Layer 2)
8	Enkapsulacija	Vsak sloj doda svojo glavo: TCP, IP, Ethernet → nastane okvir, ki potuje po omrežju.	OSI / TCP-IP
9	Prenos podatkov	Fizični sloj prenese podatke kot električne ali radijske signale.	UTP, Wi-Fi
10	Deenkapsulacija in prikaz	Strežnik pošlje odgovor; brskalnik odstrani sloje, interpretira HTML in prikaže vsebino.	TLS/HTTP/HTML

14.3 Povezava s konceptom varnosti

Vsaka faza komunikacije ima tudi svoj varnostni pomen.

Razumevanje teh točk pomaga pri prepoznavanju groženj in uporabi ustreznih zaščitnih ukrepov.

Tabela 31

Sloj / Proces	Tipične grožnje	Obrambni mehanizmi
DNS	DNS spoofing, cache poisoning	DNSSEC, nadzor nad resolverji
IP / NAT	IP spoofing, preusmerjanje	Filtriranje, usmerjevalni požarni zid
TCP	SYN flood, session hijacking	Rate-limiting, randomizacija sekvenc
ARP	ARP spoofing, MITM	statični ARP, IDS/IPS sistemi
MAC / Ethernet	MAC spoofing, sniffing	Port security, VLAN segmentacija
Enkapsulacija / TLS	prestrezanje podatkov	Šifriranje (TLS/SSL), HTTPS
Aplikacijski sloj	Phishing, XSS, zlonamerna vsebina	Varnostne posodobitve, filtriranje

14.4 Shema poteka

```
Uporabnik → Brskalnik → DNS → TCP/IP → NAT → ARP → MAC → Fizični prenos →
Strežnik
                                                          ↓
                                                Odgovor / HTML vsebina
```

V procesu vsak protokol prevzame določeno funkcijo, od prevoda imen do fizične dostave, kar omogoča zanesljivo komunikacijo med tisoči naprav po svetu.

Vaja 1 – Opazuj celoten potek v Wiresharku

1. Zaženi **Wireshark**.
2. V brskalnik vpiši:
   https://fl.um.si
3. Nato uporabi naslednje filtre in jih opazuj v tem vrstnem redu:
   - dns – poizvedba za IP naslov,
   - tcp.handshake – vzpostavitev povezave,
   - tls – šifrirana seja HTTPS,
   - arp – preslikava IP ↔ MAC,
   - eth – fizični prenos okvirov.
4. V vsakem koraku označi:
   - IP pošiljatelja in prejemnika,
   - uporabljena vrata,
   - protokol sloja.

Vaja 2 – Izris komunikacijskega diagrama

Na podlagi prejšnje vaje nariši pot podatkov od svojega računalnika do spletnega strežnika.

Vključi naslednje elemente:

- tvoj računalnik (notranji IP, MAC),
- usmerjevalnik (NAT pretvorba),
- strežnik (zunanji IP),
- sloje: **DNS, TCP/IP, Ethernet**.
  Označi, kje se pojavi enkapsulacija in kje deenkapsulacija.

Vaja 3 – Razmislek

Odgovori na vprašanja:

1. Kateri protokol bi prvi odpovedal, če bi DNS ne deloval?
2. Zakaj NAT ščiti notranje omrežje pred zunanjimi povezavami?
3. Kako bi zaznal ARP spoofing v lokalnem omrežju?

4. Zakaj je TLS pomemben pri enkapsulaciji podatkov?

14.5 Povzetek

Tabela 32

Pojem	Pomen
Enkapsulacija	Ovijanje podatkov z glavo posameznega sloja
Deenkapsulacija	Odstranjevanje teh slojev pri prejemniku
DNS	Pretvarja imena v IP naslove
TCP / IP	Urejata povezavo in prenos podatkov
NAT	Pretvarja zasebne naslove v javne
ARP / MAC	Zagotavljata dostavo znotraj lokalnega omrežja
Ethernet / fizični sloj	Skrbita za dejanski prenos bitov
TLS / HTTPS	Zagotavlja zaupnost in integriteto prenosa

Univerzitetna založba
Univerze v Mariboru

15 Orodja

Predlagana orodja za vaje

Tabela 33

Namen	Orodje	Uporaba
Osnovna diagnostika	ping, tracert / traceroute	Preverjanje povezljivosti, ICMP (v4 in v6), analiza poti
IP konfiguracija	ipconfig / ifconfig / ip addr	Pregled omrežnih nastavitev, gateway, DNS, IPv6
Lokalni ARP	arp -a / ip neigh	Preverjanje MAC–IP vezav, lokalne topologije
DNS analiza	nslookup, dig	Preverjanje domen, MX/SPF/TXT zapisov, reverse DNS
Port scanning	Nmap	TCP/UDP port scan, odkrivanje storitev, skripte (npr. SMB, SNMP)
Prometni zajem	Wireshark / tcpdump	Analiza DNS, TCP handshake, HTTP, ARP, ICMPv6, DHCP
Aplikacijski testi	curl, telnet, nc (netcat)	Preverjanje HTTP/HTTPS, SMTP, FTP, SMB vrat in odzivov
DHCP preverjanje	ipconfig /renew, dhclient -v	Diagnostika dodeljevanja IP naslovov
IPv6 analiza	ping6, traceroute6, tcpdump icmp6	NDP, Router Advertisements, echo requests

Zaporedje uporabe orodij:

- **ipconfig / ARP** → lokalni nivo (L2–L3),
- **ping / tracert** → povezljivost (ICMP, routing),
- **nslookup / dig** → DNS razreševanje,
- **curl / telnet / nc** → aplikacijski protokoli,
- **Wireshark** → analiza paketov na vseh plasteh.

15.1 Notepad ++ (https://notepad-plus-plus.org/)

Notepad++ je brezplačen in odprtokoden urejevalnik besedil, namenjen predvsem delu z izvorno kodo in konfiguracijskimi datotekami. Deluje v okolju Windows in je priljubljen zaradi svoje hitrosti, enostavne uporabe ter širokega nabora funkcionalnosti. Uporablja ga veliko programerjev, sistemskih skrbnikov in študentov za pisanje skript, urejanje nastavitev in pregledovanje različnih vrst datotek.

Med pomembnejše zmogljivosti orodja spadajo:

- poudarjanje skladnje (syntax highlighting) za številne programske jezike, kar omogoča boljšo preglednost kode,
- več zavihkov za hkratno urejanje več dokumentov,
- iskanje in zamenjava z regularnimi izrazi, kar močno pospeši delo z večjimi besedili,
- samodejno zapiranje oklepajev in zamikanje kode, kar pomaga pri pisanju skript in programov,
- podpora za vtičnike (plug-ins), s katerimi lahko dodajamo nove funkcije, kot so FTP dostop, preverjanje slovnice ali pretvorbe formatov.

Notepad++ je izjemno uporabno orodje pri tehničnih vajah, saj omogoča hitro in pregledno urejanje PowerShell skript, XML datotek, HTML strani, konfiguracijskih datotek in drugih besedilnih formatov. Zaradi majhne velikosti in hitrega zagona je priročen tudi za uporabo na šolskih računalnikih ali prenosnikih z omejenimi viri.



Pomni!

Čeprav je Notepad++ naprednejši od osnovnega Beležnice (Notepad), ne deluje kot polnopravno razvojno okolje (IDE). Njegova prednost je preprostost in prilagodljivost, kar ga naredi odličnega za učenje in osnovno delo s kodo.



Primer v praksi

Pri pisanju PowerShell skripte za izračun SHA-256 lahko datoteko hitro odpremo v Notepad++, uredimo pot do datoteke, shranimo spremembe in skripto takoj zaženemo v PowerShell okolju. Pregledno barvno označevanje ukazov olajša razumevanje in odpravljanje napak.

15.2 Sublime Text (https://www.sublimetext.com/)

Sublime Text je izjemno zmogljiv in hiter večplatformski besedilni urejevalnik, zasnovan za učinkovito delo s kodo, vključno z HTML. Cenjen je med profesionalnimi razvijalci in študenti zaradi svoje hitrosti in bogatega nabora funkcij.

Za razliko od osnovnega Notepada, Sublime Text nudi napredno okolje za pisanje čistega in veljavnega HTML-ja.

Med pomembnejše zmogljivosti orodja spadajo:

- sintaktično poudarjanje (Syntax highlighting), ki omogoča vizualno ločevanje oznak, atributov in besedila, s tem pa boljšo preglednost kode,
- široka podpora za različne programske jezike in tipe datotek,
- zavihki za hkratno urejanje več povezanih dokumentov (npr. index.html, kontakt.html),
- organizacija projektov, ki omogoča, da celotno strukturo mape (datoteke in podmape) odpremo in upravljamo v enem oknu in
- napredna orodja za delo s kodo, ki pripravijo študenta na razvoj zahtevnejših spletnih sistemov.

Sublime Text je odlično orodje za uvodne vaje v HTML, saj združuje preprostost s poudarjanjem kode, kar olajša prepoznavanje in odpravljanje sintaktičnih napak.



Pomni!

Tudi Sublime Text je primarno urejevalnik kode in ne polnopravno razvojno okolje (IDE). Njegova uporaba pri pisanju HTML omogoča učinkovito in pregledno urejanje kode, s poudarkom na pravilni strukturi, ne da bi koda postala preveč kompleksna.



Primer v praksi

Pri ustvarjanju mini-projekta s tremi povezanimi podstranmi (index.html, tabela.html, kontakt.html), nam Sublime Text omogoči, da imamo vse tri datoteke odprte v zavihkih in hkrati vidimo celotno strukturo projekta ob strani. To omogoča hitro preklapljanje med stranmi in preverjanje, ali se ustrezne povezave (<a href="kontakt.html">) pravilno ujemajo.

15.3 Wireshark (https://www.wireshark.org/)

Wireshark je brezplačno in odprtokodno orodje za analizo omrežnega prometa (packet analyzer), ki omogoča zajem in podroben pregled vseh podatkovnih paketov, ki potekajo skozi omrežni vmesnik. Uporablja se pri izobraževanju, raziskavah in vsakdanjem delu sistemskih skrbnikov, omrežnih in varnostnih strokovnjakov.

Deluje v okoljih **Windows, Linux in macOS** ter podpira številne omrežne protokole (TCP, UDP, ICMP, DNS, HTTP, ARP, NAT, SSL/TLS …). Njegova prednost je, da omogoča vpogled v dogajanje "pod površjem" – kako računalniki dejansko komunicirajo prek omrežja.

Med pomembnejše zmogljivosti orodja spadajo:

- zajem prometa v realnem času z možnostjo filtriranja po protokolih, IP-jih, vratih ali ključnih besedah,
- podrobna analiza vsakega paketa: izvor, cilj, protokol, dolžina, vsebina in čas pošiljanja,
- barvno označevanje različnih vrst prometa (npr. DNS, TCP, ICMP), kar povečuje preglednost zajema,
- uporaba naprednih filtrov (Display Filter) za hitro iskanje določenih dogodkov ali komunikacij,
- možnost shranjevanja in ponovnega odpiranja zajetih sej (.pcap datoteke) za kasnejšo analizo ali primerjavo,
- podpora za dekodiranje številnih protokolov in TLS sej (če so na voljo ključi), kar omogoča poglobljeno varnostno analizo.

Wireshark je nepogrešljivo orodje pri tehničnih vajah, saj omogoča praktično opazovanje, kaj se dogaja od trenutka, ko v brskalnik vpišemo spletni naslov, do trenutka, ko se stran prikaže. Študenti lahko v živo spremljajo DNS poizvedbe, TCP povezave, ARP zahteve in ICMP odzive ter jih povežejo s teoretičnim znanjem iz posameznih poglavij.



Pomni!

Wireshark zahteva zavedanje o etičnih in varnostnih vidikih: zajemanje prometa je dovoljeno le v lastnem ali za to odobrenem omrežju. Orodje ni namenjeno prestrezanju podatkov drugih uporabnikov.



Primer v praksi

Pri analizi dostopa do spletne strani https://fl.um.si lahko v Wiresharku uporabimo filter dns za opazovanje iskanja domenskega imena, nato tcp.port == 443 za spremljanje vzpostavitve varne HTTPS seje. Študent lahko prepozna faze TCP handshake-a, preveri IP naslov strežnika in razume, kako poteka komunikacija med brskalnikom in strežnikom v resničnem času.

Univerzitetna založba
Univerze v Mariboru

16 Sklep

V prejšnjih poglavjih smo spoznali, kako se v manj kot eni sekundi odvije kompleksen proces, ko v brskalnik vpišemo spletni naslov. Za tem preprostim dejanjem se skriva prepleten sistem protokolov, naprav, naslovov in mehanizmov, ki skupaj tvorijo osnovo delovanja interneta.

Razumevanje teh procesov ni zgolj tehnična vaja, temveč temeljno znanje za vsakega strokovnjaka s področja informacijske tehnologije in varnosti.

Vsak korak, od pretvorbe domene v IP naslov do pretoka električnih signalov po fizičnem mediju, odpira vprašanja zanesljivosti, učinkovitosti in zaščite podatkov.

Skozi DNS spoznamo pomen zaupanja v infrastrukturo interneta, saj napačen ali zlonamerno spremenjen zapis lahko preusmeri celotno komunikacijo. TCP in port number učita, kako računalniki vzpostavljajo in nadzorujejo povezave, medtem ko NAT pokaže, kako si lahko milijoni naprav delijo omejen naslovni prostor. ARP in MAC nas popeljeta na fizično raven, kjer se podatki prenašajo med resničnimi napravami, enkapsulacija pa razkrije, kako vse te ravni sodelujejo v enotni strukturi komunikacije.

Pomemben del razumevanja teh procesov je tudi varnostni vidik.

Vsaka plast omrežja ima svoje ranljivosti, od zastrupljenih DNS predpomnilnikov in lažnih ARP odgovorov do napadov na TCP seje in prestrezanja podatkov na fizični ravni. Zato mora biti vsaka analiza tehničnega delovanja dopolnjena z zavedanjem, kako se zlorabe preprečujejo: z varnimi konfiguracijami, šifriranjem, preverjanjem pristnosti in stalnim spremljanjem omrežnih dogodkov.

Učbenik se tako ne ustavi le pri opisu tehnologij, temveč želi razviti celostno razumevanje omrežnih procesov: od logike delovanja do pomena odgovorne in varne uporabe informacijskih sistemov. Razumevanje poti »od URL do prikaza« omogoča študentu, da vidi informacijsko okolje kot živi sistem, kjer se teorija in praksa nenehno prepletata.

Na koncu velja poudariti, da se vloga poznavanja omrežnih osnov v digitalni družbi še krepi.

Vsak klik, vsaka zahteva do strežnika, vsaka povezava Wi-Fi predstavlja verigo, v kateri mora vsak člen delovati varno in zanesljivo. Če to razumemo, smo naredili prvi korak k temu, da ne uporabljamo interneta le kot uporabniki, temveč kot odgovorni graditelji digitalnega sveta.

Univerzitetna založba
Univerze v Mariboru

Viri

Berners-Lee, T., Masinter, L. M. in McCahill, M. P. (1994). Uniform Resource Locators (URL) (RFC 1738). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc1738

Deering, S. in Hinden, R. (2017). Internet Protocol, version 6 (IPv6) specification (RFC 8200). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc8200

Mockapetris, P. (1987a). Domain names – Concepts and facilities (RFC 1034). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc1034

Mockapetris, P. (1987b). Domain names – Implementation and specification (RFC 1035). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc1035

Postel, J. (1981a). Internet Control Message Protocol (RFC 792). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc792

Postel, J. (1981b). Internet Protocol (RFC 791). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc791

Rekhter, Y., Moskowitz, R., Karrenberg, D., de Groot, G. J. in Lear, E. (1996). Address allocation for private internets (RFC 1918). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc1918

Reynolds, J. (1992). Assigned numbers (RFC 1340). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc1340

Srisuresh, P. in Holdrege, M. (1999). IP Network Address Translator (NAT) terminology and considerations (RFC 2663). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc2663

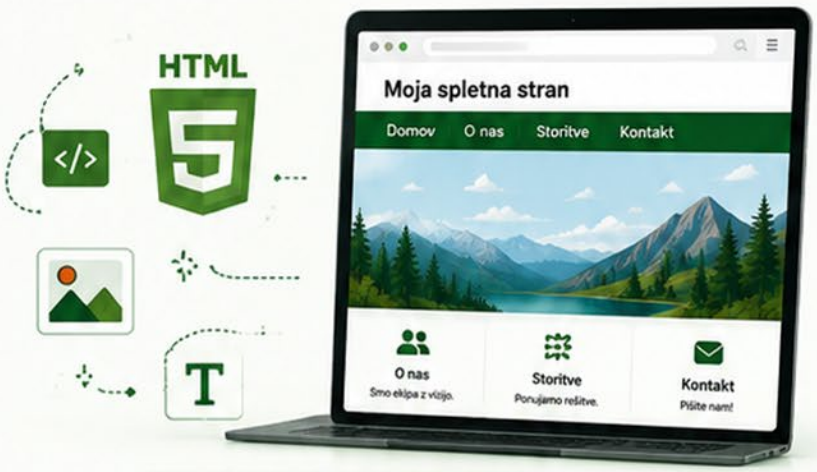
Touch, J. (2013). Updated specification of the IPv4 ID field (RFC 6864). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc6864

Woodburn, R. in Mills, D. L. (1991). A scheme for an internet encapsulation protocol: Version 1 (RFC 1241). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc1241

2. SKLOP
HTML

Od kode do spletne strani: struktura, oznake in vsebina

HTML (HyperText Markup Language) je jezik, s katerim strukturiramo in označimo vsebino spletne strani. Brskalnik kodo HTML pretvori v berljivo in privlačno spletno stran, ki jo vidimo na zaslonu.



OSNOVA HTML DOKUMENTA

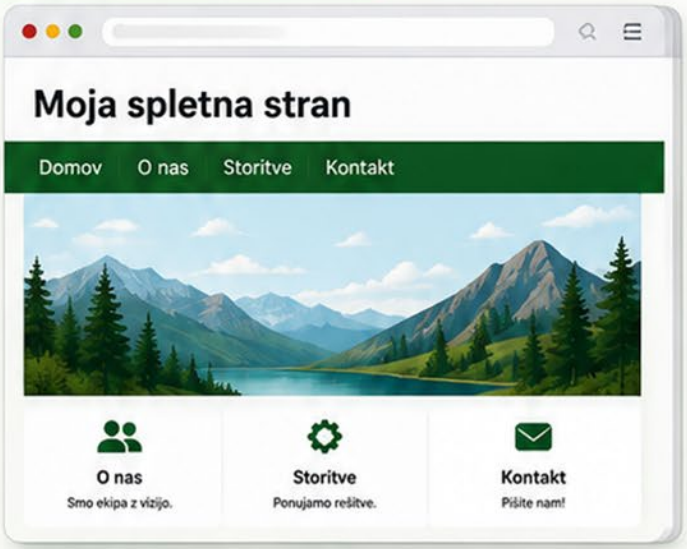
<head>
Informacije za brskalnik (naslov, kodiranje, metapodatki, ...)

<body>
Vsebina, ki je vidna uporabniku

```
1  <!DOCTYPE html>
2  <html lang="sl">
3  <head>
4    <meta charset="UTF-8">
5    <title>Moja spletna stran</title>
6  </head>
7  <body>
8     <h1>Dobrodošli!</h1>
9     <p>To je primer spletne strani,</p>
10    <p>izdelane s HTML.</p>
11  </body>
12 </html>
```

HTML tags (oznake) so obdane z oglatimi oklepaji < >.
Večina oznak ima odprto in zaprto obliko: <oznaka> ... </oznaka>.

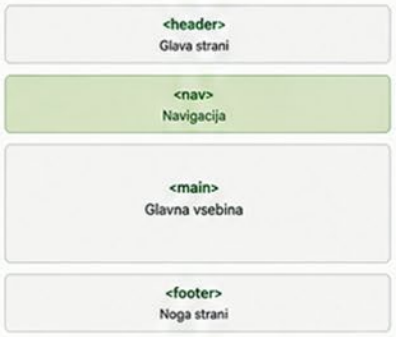
PRIMER REZULTATA V BRSKALNIKU



POMEMBNE HTML OZNAKE

T	<h1>–<h6>	Naslov	Naslovi različnih stopenj (h1 je najpomembnejši)
¶		Odstavek besedila.	Odstavek besedila
🔗	<a>	UM	Povezava do druge strani
🖼	<img>	<img src="slika.jpg" alt="Slika">	Vstavi sliko (alt opis za dostopnost)
☰	/ /	- Prvi - Drugi	Seznami – nenumerirani (ul), numerirani (ol), postavka (li)
▦	<table>	<table>...</table>	Tabele za strukturirane podatke
▭	<form>	<input type="text" name="ime">	Obrazci za vnos podatkov
</>	<header> <nav> <main> <footer>	<header>...</header>	Semantični elementi za boljšo berljivost in dostopnost

SEMANTIČNA STRUKTURA STRANI



DOSTOPNOST
Razumljivejše osebam z invalidnostjo.

SEO OPTIMIZACIJA
Iskalniki bolje razumejo strukturo vsebine.

VZDRŽEVANJE
Koda je preglednejša in lažje vzdrževana.

POSTOPEK IZDELAVE SPLETNE STRANI



1. Načrtuj strukturo in vsebino.
2. Napiši HTML kodo v urejevalniku (npr. VS Code).
3. Preveri kodo z W3C validatorjem (htmlvalidator.com).
4. Preizkusi v brskalniku (Chrome, Firefox ...).
5. Objavi na strežnik ali lokalno (preko XAMPP).

VALIDACIJA KODE – W3C

Preveri pravilnost HTML kode na uradni strani W3C:

https://validator.w3.org

Veljavna koda = manj napak, boljša združljivost in dostopnost.

PRIMER POGOSTIH NAPAK

- Pozabljena zaprta oznaka: Besedilo
- Nepravilno gnezdenje oznak
- Nezakonski atributi ali vrednosti
- Manjkajoči alt pri slikah



DOBRE PRAKSE PRI PISANJU HTML

- Uporabljaj semantične oznake.
- Piši berljivo in urejeno kodo.
- Dodaj alt besedila za slike.
- Uporabljaj smiselne povezave in naslove.
- Ne objavljaj občutljivih podatkov na spletni strani.
- Misli na uporabnika – jasna struktura in preglednost.

Univerzitetna založba
Univerze v Mariboru

1 Uvod

Zgodba o brskanju se je končala v trenutku, ko je brskalnik odstranil vse omrežne plasti in mu je v rokah ostal le še HTML. A prav tu se začne nova zgodba. Datoteka, ki je pripotovala s strežnika, je navadno besedilo — brez barv, brez slik, brez postavitve. Če bi jo odprl v Beležnici, bi videl le nize oznak, zapisanih med lomljenima oklepajema: <h1>, <p>, <a>. Prav te neugledne oznake pa brskalniku povedo vse, kar potrebuje, da iz golega besedila sestavi urejeno spletno stran z naslovi, odstavki, povezavami in slikami.

HTML (angl. *HyperText Markup Language*) ni programski jezik, temveč označevalni jezik: ne vsebuje logike, pogojev ali zank, ampak vsebini pripisuje pomen in strukturo. Oznaka <h1> brskalniku ne pove, kako naj bo naslov videti, temveč da je to najpomembnejši naslov na strani. Ta na videz drobna razlika — ločevanje pomena vsebine od njenega videza — je eden temeljnih konceptov sodobnega spleta. Hkrati pa je tudi razlog, da isto stran enako dobro razumejo brskalnik na telefonu, iskalnik, ki jo uvršča med zadetke, in bralnik zaslona, ki jo prebere slepemu uporabniku.

Ta jezik je leta 1989 v laboratoriju CERN zasnoval fizik Tim Berners-Lee, ko je iskal način, kako bi si znanstveniki izmenjevali dokumente med različnimi računalniki. Prva različica je poznala le naslove, odstavke, sezname in povezave. A prav povezave (hiperpovezave) so bile revolucionarna zamisel, ki je posamezne dokumente spletla v svetovni splet. Skozi desetletja se je jezik razvijal do današnjega standarda HTML5, ki poleg besedila obvlada tudi video, zvok, obrazce in semantične razdelke, pravila zanj pa določa konzorcij W3C (World Wide Web Consortium, 2025), in sicer tako, da vsebino vsi brskalniki razumejo enako.

V tem sklopu boš HTML spoznal od znotraj. V navadnem urejevalniku, kot je Beležnica, boš zgradil svoj prvi veljaven dokument, ga preveril s spletnim validatorjem W3C, nato pa mu korak za korakom dodajal naslove, povezave, slike, sezname, tabele in obrazce, dokler

ne bo nastala prava mala spletna stran z več povezanimi podstranmi. Ob tem boš videl, da za razumevanje spleta ne potrebuješ dragih orodij — le natančnost, doslednost in razumevanje strukture.

Znanje HTML pa ni pomembno le za tiste, ki bodo spletne strani izdelovali. V organizacijah in logističnih okoljih se s HTML srečamo povsod: v spletnih portalih za sledenje pošiljk, v samodejno ustvarjenih e-poštnih sporočilih, v spletnih obrazcih za naročila. Kdor razume, kaj se skriva za prikazano stranjo, zna presoditi, katere podatke je varno objaviti, prepozna ponarejen obrazec, ki krade podatke, in razume, zakaj je premišljena struktura informacij temelj tako dobre uporabniške izkušnje kot tudi informacijske varnosti.

Univerzitetna založba
Univerze v Mariboru

2 Kaj je HTML

HTML (angl. *HyperText Markup Language* — jezik za označevanje hiperteksta) je osnovni gradnik vseh spletnih strani.

Z njim **opisujemo strukturo in pomen vsebine**, ki jo brskalnik prikaže uporabniku.

HTML **ni programski jezik**, temveč **označevalni jezik** — to pomeni, da ne vsebuje logike (pogojnih stavkov, zank ipd.), ampak uporablja **oznake (elemente)** za označevanje vsebine, npr.:

```
<p>To je odstavek.</p>
<h1>To je naslov.</h1>
<a href="https://www.um.si">Povezava</a>
```

Vsaka oznaka ima **začetek** in **konec**, med njima pa je besedilo ali drug element.

2.1 Kako je HTML nastal

HTML je nastal konec 80. in v začetku 90. let kot del prve zamisli svetovnega spleta Berners-Lee in Connolly, 1995).

Ustvaril ga je **Tim Berners-Lee**, fizik v laboratoriju **CERN** (Švica), leta **1989**, ko je iskal način, kako bi znanstveniki med seboj izmenjevali dokumente na različnih računalnikih.

Prva verzija **HTML 1.0** (okrog leta 1991) je omogočala le:

- naslove,
- odstavke,

- sezname in
- povezave (angl. *hyperlinks*).

Kasneje so se dodali:

- tabele (HTML 3.2),
- okvirji (angl. *frames*),
- obrazci,
- slogovne oznake,
- in nazadnje (v **HTML5**) podpora za **video, audio, semantične oznake** in **dostopnost**.

Današnja različica — **HTML5** — je standardizirana pri **W3C (angl. *World Wide Web Consortium*)**, ki določa pravila, kako morajo brskalniki prikazovati vsebino.

2.2 Zakaj uporabljamo HTML?

HTML omogoča:

1. **Strukturirano predstavitev informacij** – vsebina je razdeljena na naslove, odstavke, sezname, tabele, slike ...
2. **Medsebojno povezanost** – povezave (*links*) povezujejo dokumente v spletno mrežo (angl. *web*).
3. **Dostopnost in medopravilnost** – pravilno napisan HTML je berljiv za ljudi, računalnike in pomočnike (npr. bralnike zaslona).
4. **Temelj varnega spletnega objavljanja** – pravilna struktura omogoča nadzor, preverjanje (validatorje) in varno vgradnjo drugih vsebin (CSS, JavaScript).

2.3 Kaj pomeni izraz “obogateno besedilo”?

Obogateno besedilo (angl. *Hypertext*) pomeni besedilo, ki vsebuje **povezave na druge dokumente**.

Zato HTML ni samo “besedilo na zaslonu”, ampak mreža dokumentov, povezanih z `<a href="...">`.

Primer:

```
<p>Več informacij najdete na <a href="https://www.w3.org">spletnem
mestu W3C</a>.</p>
```

Klik povezave odpre drug dokument – to je bistvo spleta.

2.4 Kako deluje brskalnik?

Ko odpremo datoteko index.html, brskalnik:

1. prebere HTML kodo,
2. ustvari **strukturo dokumenta** (t. i. *Document Object Model – DOM*),
3. prikaže vsebino uporabniku.

Če HTML vsebuje napake (npr. manjkajoče oznake), poskuša brskalnik ugibati, kako jih zapreti – zato je pomembno pisati **čist in veljaven** HTML.

2.5 Kako se HTML vključi v kontekst informatike in varnosti?

V okviru predmeta Informatika in informacijska varnost v organizacijah ima HTML več pomenov:

- je **osnova digitalne komunikacije** med organizacijami (spletne strani, portali, dokumentacija);
- z njegovo pomočjo se **pravilno strukturirani podatki** (npr. poročila, tabele, kontakti) varno prikazujejo;
- pravilna raba oznak in metapodatkov izboljša **sledljivost in preglednost informacij**;
- omogoča **nadzor nad objavami**, s čimer se zmanjšajo napake in tveganja (npr. objava napačnih ali zasebnih podatkov).

2.6 Datoteka HTML

V grobem je HTML dokument sestavljen iz dveh osnovnih delov: glave (angl. *head*) in telesa (angl. *body*). Glava vsebuje informacije o dokumentu, ki jih potrebujejo brskalniki in drugi programi (na primer naslov strani, uporabljeno kodiranje znakov in druge metapodatke), telo pa vsebuje vsebino, ki jo uporabnik vidi na zaslonu. Takšna ločitev med opisnimi podatki in vsebino ni značilna le za HTML, temveč jo srečamo tudi pri

drugih zapisih podatkov, na primer v XML dokumentih. Podrobneje si bomo zgradbo HTML dokumenta ogledali v naslednjem poglavju.

Datoteka HTML je običajna znakovna datoteka, kar pomeni, da jo lahko odpremo in urejamo s poljubnimi urejevalniki besedil. Datoteke v HTML imajo končnico .htm ali .html, pišemo pa jih v besedilnem urejevalniku, lahko pa uporabimo katerega od zmogljivejših orodij, ki npr. barvajo izvorno kodo ali pa nam nudijo nabor trenutno možnih ukazov, lahko pa celo sproten pogled na izdelek.

2.7 Prvi koraki v praksi

Za delo z HTML ne potrebujemo posebnih programov — zadošča:

- ***Notepad*** (ali *Notepad++*),
- in **spletni brskalnik** (npr. *Chrome, Firefox, Edge*).

1. Ustvari datoteko index.html.
2. Vpiši osnovno strukturo:

```
<!DOCTYPE html>
<html lang="sl">
<head>
  <meta charset="UTF-8">
  <title>Moja prva stran</title>
</head>
<body>
  <h1>Pozdrav, svet!</h1>
</body>
</html>
```



Shrani in odpri v brskalniku — to je tvoja prva spletna stran.

2.8 Uporaba različnih orodij

Za delo z HTML ne potrebujemo posebnih programov — zadošča:

- ***Notepad*** (ali *Notepad++*),
- in **spletni brskalnik** (npr. *Chrome, Firefox, Edge*).

Datoteka HTML je običajna znakovna datoteka, kar pomeni, da jo lahko odpremo in urejamo s poljubnimi urejevalniki besedil. Datoteke v HTML imajo končnico **.htm** ali **.html**.

Pišemo jih lahko v besedilnem urejevalniku, lahko pa uporabimo katerega od zmogljivejših orodij, ki na primer:

- barvajo izvorno kodo,
- nudijo nabor trenutno možnih ukazov,
- ali celo sproten pogled na izdelek.

2.8.1 Notepad: Vaš prvi HTML urejevalnik

Notepad (Beležnica) je enostaven, a zmogljiv besedilni urejevalnik, vgrajen v operacijski sistem Windows, ki služi kot idealno orodje za učenje in pisanje vaše prve kode HTML.

Zakaj uporabljamo Notepad?

1. **Enostavnost in dostopnost:** Notepad je **znakovna datoteka** (tekstovna datoteka), kar pomeni, da je popolnoma brez vseh funkcij za oblikovanje, ki jih imajo programi, kot je *Microsoft Word*. Za delo z HTML ne potrebujete posebnih programov – zadošča že Notepad in spletni brskalnik (npr. *Chrome, Firefox, Edge*).
2. **Fokus na kodo:** Ker *Notepad* ne dodaja nobene skrite oblike ali logike, se lahko popolnoma osredotočite na **strukturo, logiko in pravilno rabo jezika HTML**. To je bistveno za razumevanje, kako brskalnik prebere in prikaže vsebino.
3. **Temelj spletnega ustvarjanja:** S pomočjo *Notepada* se naučite osnovnih korakov: vnašanja čiste kode, shranjevanja datoteke s pravilno končnico (**.htm** ali **.html**) in odpiranja v brskalniku, kar je temelj vsake spletne strani.

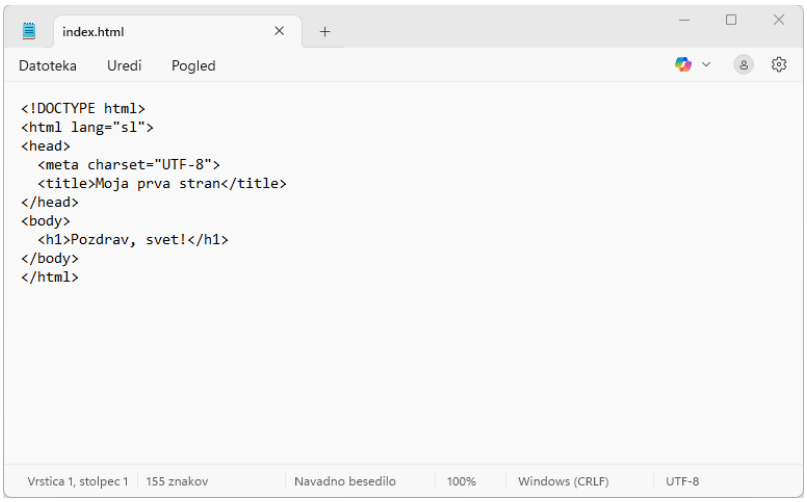
Kako ustvariti prvi dokument v Notepadu?

1. **Odpiranje Notepada:** Začnete z odprtjem programa *Notepad* na vašem računalniku.
2. **Vnos osnovne Sstrukture:** V prazno okno vnesete osnovno strukturo dokumenta HTML5:

```
HTML
<!DOCTYPE html>
<html lang="sl">
<head>
```

```
<meta charset="UTF-8">
<title>Moja prva stran</title>
</head>
<body>
<h1>Pozdrav, svet!</h1>
</body>
</html>
```

3. **Shranjevanje:** Datoteko shranite z izbiro menija "Shrani kot" in ji določite ime, kot je **index.html**. Zelo pomembno je, da pri shranjevanju izberete **Kodiranje: UTF-8**, da brskalnik pravilno prebere slovenske šumnike (č, š, ž).
4. **Ogled v brskalniku:** Shranjeno datoteko index.html nato odprite s spletnim brskalnikom, kjer boste videli prikaz vaše prve spletne strani.



2.8.2 Notepad++: Zmogljivejši urejevalnik kode

Notepad++ je brezplačen urejevalnik izvorne kode, ki je namenjen programerjem in spletnim razvijalcem. Čeprav za pisanje osnovne kode HTML zadostuje že klasični *Notepad*, vam *Notepad*++ nudi številne funkcije, ki izboljšajo hitrost, berljivost in natančnost vašega dela.

Prednosti *Notepad++* pred klasičnim *Notepadom*

Notepad++ je v osnovi tekstovni urejevalnik, a ponuja dodatke, ki so zelo koristni pri pisanju HTML:

– **Barvanje izvorne kode (sintaktično poudarjanje):** različne oznake, atributi in vrednosti v kodi HTML so prikazani v različnih barvah. To močno poveča berljivost kode in vam pomaga hitro prepoznati napake ali manjkajoče elemente.

- **Številčenje vrstic:** Omogoča enostavno sledenje in iskanje napak, še posebej, ko kodo preverjate s spletnim validatorjem W3C, ki pogosto navaja napake po številkah vrstic.
- **Zavihki (angl. *Tabs*):** Omogoča vam, da imate hkrati odprtih in urejate več datotek (npr. index.html, onas.html, kontakt.html) v enem oknu.
- **Samodejno dokončanje (Avtokompletiranje):** Nudi vam nabor trenutno možnih ukazov oziroma oznak.

Delo z HTML v *Notepadu++*

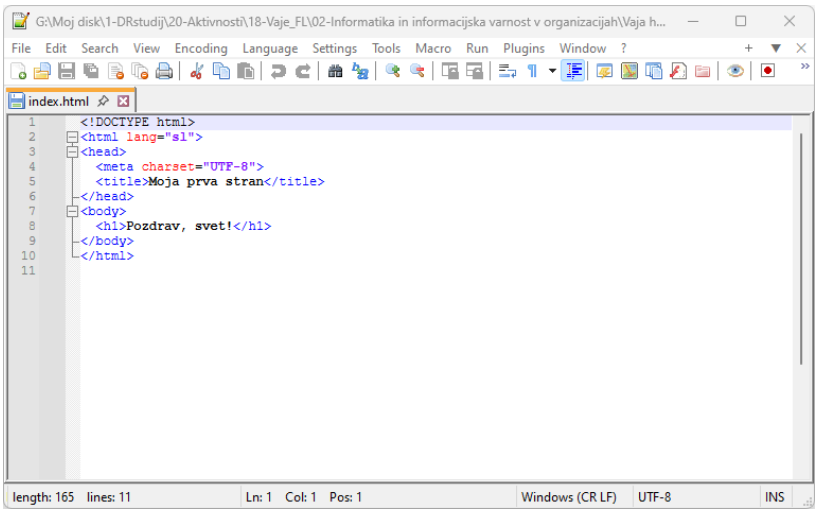
Pri uporabi *Notepad*++ so koraki za ustvarjanje datoteke HTML enaki kot pri klasičnem Notepadu, vendar je delo preglednejše:

1. **Vnos kode:** Vnesete osnovno strukturo dokumenta HTML5:

```
HTML
<!DOCTYPE html>
<html lang="sl">
<head>
<meta charset="UTF-8">
<title>Uvod v HTML</title>
</head>
<body>
<h1>Moja prva stran</h1>
</body>
</html>
```

2. **Sintaktično poudarjanje:** Ko datoteko shranite s končnico **.html**, *Notepad*++ samodejno prepozna, da gre za HTML, in obarva kodo.
3. **Shranjevanje:** Poskrbite, da je kodiranje nastavljeno na **UTF-8**, da se pravilno prikažejo vsi znaki, vključno s šumniki (č, š, ž).

Uporaba urejevalnika, kot je *Notepad*++, vas postopoma uvaja v naprednejše okolje, ki ga boste potrebovali pri kasnejšem delu z večjimi spletnimi sistemi in ločevanju vsebine (HTML) od oblikovanja (CSS).



2.8.3 *Sublime Text*: Zmogljiv in prilagodljiv urejevalnik kode

Sublime Text je priljubljen, večplatformski urejevalnik besedil in izvorne kode, ki je med razvijalci cenjen zaradi svoje hitrosti, zmogljivosti in izjemne prilagodljivosti. Za razliko od Notepada, ki je osnovno orodje, je *Sublime Text* orodje, ki vas pripravi na razvoj zahtevnejših spletnih sistemov.

Prednosti *Sublime Texta* pri pisanju HTML

Sublime Text v primerjavi s klasičnim *Notepadom* prinaša bistvene izboljšave, ki močno pospešijo učenje in delo:

- **Sintaktično poudarjanje in samodejno dokončanje (angl. *IntelliSense*):** *Sublime Text* avtomatsko prepozna jezik HTML in obarva oznake, atribute in besedilo. Hkrati vam pri vnašanju kode predlaga možne oznake in atribute (npr. ko vnesete <h, predlaga <h1>, <h2> itd.), kar zmanjša število napak in pospeši delo.
- **Organizacija projekta:** Omogoča vam, da celotno mapo z vajami (npr. moj-projekt/ z datotekami index.html, kontakt.html in mapo images/) odprete kot **projekt**. To v oknu urejevalnika prikaže strukturo datotek, kar olajša premikanje med povezanimi podstranmi.
- **Več vrstic (angl. *Multi-Cursor Editing*):** Ta napredna funkcija omogoča urejanje več nepovezanih vrstic ali delov kode hkrati. To je izjemno uporabno, kadar morate v več datotekah ali delih ponavljati enake spremembe.
- **Videz (angl. *Theme*) in prilagodljivost:** Za delo v slabših svetlobnih pogojih ali za manj utrujanja oči nudi možnost temnega vmesnika, ki je prijaznejši za daljše urejanje kode .

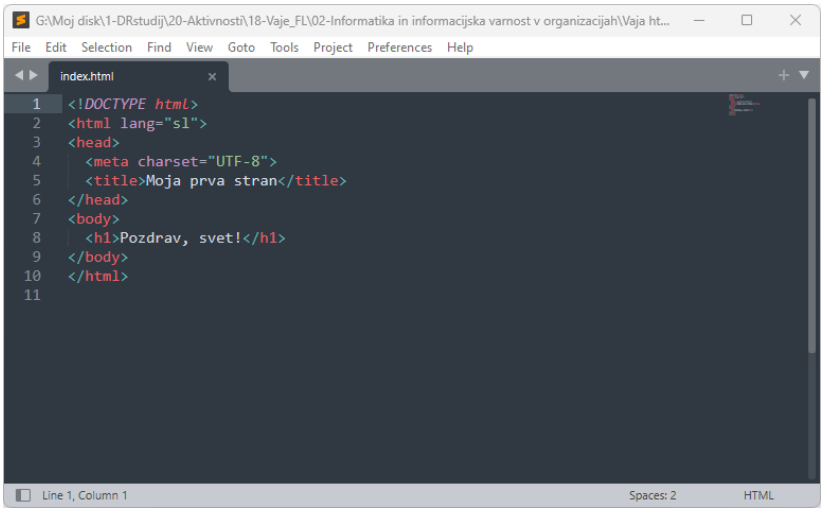
Uporaba *Sublime Texta* za uvodno HTML kodo

1. **Vnos osnovne strukture:** Vnesite kodo, kot je:

```
HTML
<!DOCTYPE html>
<html lang="sl">
<head>
<meta charset="UTF-8">
<title>Uvod v Sublime Text</title>
</head>
<body>
<h1>Moja prva spletna stran</h1>
</body>
</html>
```

2. **Delo in shranjevanje:** Program samodejno ponuja shranjevanje v kodiranju **UTF-8**, kar zagotavlja pravilno prikazovanje šumnikov. Shranite datoteko s končnico **.html**.

Sublime Text je idealen za študente, ki želijo preiti od osnovnih principov k učinkovitemu in strokovnemu pisanju čiste, veljavne kode HTML.



Univerzitetna založba
Univerze v Mariboru

3 Osnovna zgradba HTML dokumenta

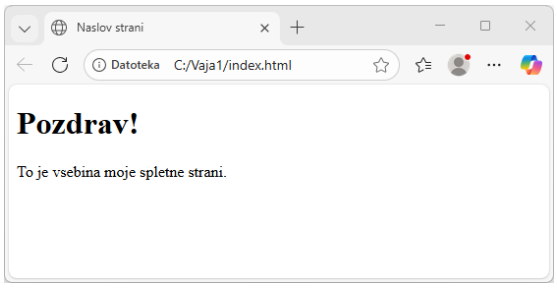
3.1 Osnovna ideja

Vsaka spletna stran v jeziku HTML ima **vedno enako osnovno strukturo**.

Ta struktura pove brskalniku, kako je dokument zgrajen, kateri jezik uporablja in kako naj se vsebina prikaže uporabniku.

Osnovna oblika vsake datoteke HTML je:

```
<!DOCTYPE html>
<html lang="sl">
<head>
  <meta charset="UTF-8">
  <title>Naslov strani</title>
</head>
<body>
  <h1>Pozdrav!</h1>
  <p>To je vsebina moje spletne strani.</p>
</body>
</html>
```



3.2 Vloga posameznih delov

3.2.1 Deklaracija

Ta vrstica **ni oznaka**, ampak deklaracija, ki pove brskalniku, da gre za dokument v jeziku HTML5. Uporabimo oznako <!DOCTYPE html>.

Brez nje bi starejši brskalniki lahko prikazali stran v »združljivostnem načinu« (angl. *quirks mode*), kar bi povzročilo nepravilno oblikovanje.

3.2.2 Koren

To je **koren (angl. *root*)** vsakega HTML dokumenta. Uporabimo oznako <html lang="sl">

Z atributom lang="sl" določimo **jezik vsebine** – to je pomembno za:

- bralnike zaslona (dostopnost),
- prevajalne storitve,
- iskalnike (SEO).

Celotna stran mora biti znotraj oznak <html> in </html>.

3.2.3 Glava dokumenta

Del med oznakama <head> in </head> **ni viden na sami strani**, ampak vsebuje podatke *o* strani.

Imenujemo jih **metapodatki** (angl. *metadata*).

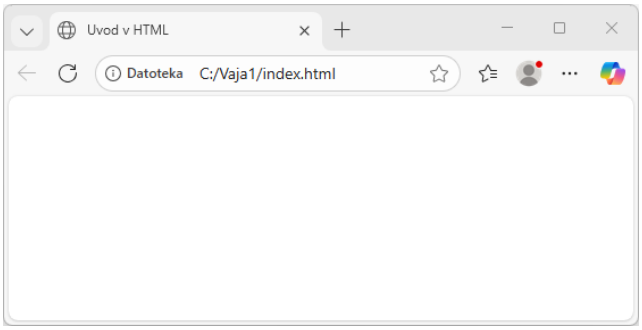
3.3 Najpogostejši elementi v glavi dokumenta

Tabela 34

Oznaka	Namen
`<title>`	Naslov strani – prikaže se v zavihku brskalnika.
`<meta charset="UTF-8">`	Določa kodiranje znakov (UTF-8 podpira tudi šumnike: č, š, ž).
`<meta name="description" content="Kratek opis strani.">`	Povzetek, ki se prikaže v iskalnikih.
`<meta name="author" content="Miha Novak">`	Avtor dokumenta.
`<link rel="icon" href="favicon.ico">`	Ikona, ki se prikaže v zavihku.

Primer:

```
<head>
  <meta charset="UTF-8">
  <meta name="author" content="Mihael Plevnik">
  <meta name="description" content="Učni primer HTML strani za logistiko.">
  <title>Uvod v HTML</title>
</head>
```



3.4 Telo dokumenta

Tukaj se nahaja **vidna vsebina spletne strani**, torej tisto, kar uporabnik vidi v brskalniku: naslovi, besedilo, slike, tabele, povezave, obrazci … Uporabimo oznako <body>.

Primer:

```
<body>
  <h1>Naslov strani</h1>
  <p>To je glavni odstavek z osnovnim besedilom.</p>
  <a href="https://www.um.si">Obišči UM</a>
</body>
```



3.5 Kako brskalnik razume HTML

Brskalnik bere dokument **od zgoraj navzdol** in vsako oznako razume kot **navodilo za prikaz**.
Če se pojavi napaka (npr. manjkajoča zaključna oznaka), brskalnik skuša uganiti, kaj si hotel zapisati — vendar rezultat ni nujno pravilen.

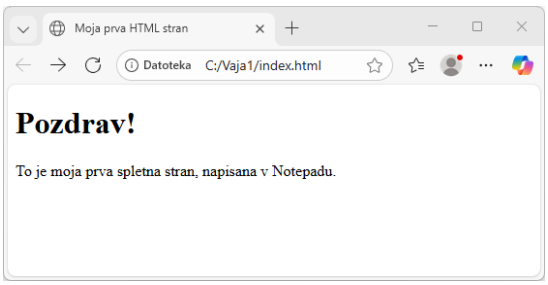
Zato vedno:

- zapiraj vse oznake (</p>, </h1> ipd.),
- preveri dokument s **HTML validatorjem**: https://validator.w3.org/.

3.6 Primer za vajo v Notepadu

1. Ustvari novo datoteko osnova.html.
2. Vpiši naslednjo kodo:

```
<!DOCTYPE html>
<html lang="sl">
<head>
  <meta charset="UTF-8">
  <meta name="author" content="Ime in priimek">
  <meta name="description" content="Uvodna vaja za predmet Informatika
in informacijska varnost.">
  <title>Moja prva HTML stran</title>
</head>
<body>
  <h1>Pozdrav!</h1>
  <p>To je moja prva spletna stran, napisana v Notepadu.</p>
</body>
</html>
```



3. Shrani datoteko in jo odpri v brskalniku.
4. Preveri, ali se naslov prikaže v zavihku in besedilo v oknu.

3.7 Povzetek

Tabela 35

Del	Vloga
`<!DOCTYPE html>`	Določa, da gre za HTML5 dokument.
`<html lang="sl">`	Začetek dokumenta in jezik.
`<head>`	Vsebuje metapodatke (nevidno vsebino).
`<body>`	Vidna vsebina strani.
`</html>`	Zaključek dokumenta.

3.8 Naloga za samostojno delo

- Ustvari datoteko index.html, kjer boš uporabil vse štiri glavne dele.
- V <body> dodaj naslov, en odstavek in eno povezavo.
- Odpri v brskalniku in preveri, ali vse deluje pravilno.
- Nato preveri veljavnost dokumenta na validator.w3.org.

3.9 Vaje za poglavje 2 – Kaj je HTML

Vaja 1: Prepoznaj HTML

Odpri katerokoli spletno stran, klikni z desno tipko miške in izberi **"Ogled izvorne kode strani" (angl. *View Page Source*)**.

1. Poišči vsaj tri oznake (npr. <html>, <head>, <body>).
2. Zapiši, kaj misliš, da vsaka od njih pomeni.
3. Prepoznaj, kje se začne in konča telo (<body>) strani.

Vaja 2: Prva koda

1. Odpri *Notepad* in vpiši naslednjo kodo:

```
<!DOCTYPE html>
<html lang="sl">
<head>
  <meta charset="UTF-8">
  <title>Moj prvi HTML</title>
</head>
<body>
  <h1>Pozdrav, svet!</h1>
```

```
    <p>To je moj prvi odstavek v jeziku HTML.</p>
</body>
</html>
```

2. Shrani kot index.html.
3. Odpri datoteko v brskalniku.
4. V razpredelnico zapiši, kateri deli kode so vidni in kateri ne.



Vaja 3: Oznake in elementi

1. V istem dokumentu dodaj še naslednje tri vrstice:

```
<h2>Podnaslov</h2>
<p>To je drugi odstavek.</p>
<a href="https://www.um.si">Povezava do UM</a>
```

2. Razloži razliko med:
   - oznako in elementom To je odstavek. ,
   - vidnim besedilom in oznako.



Vaja 4: Kdo je ustvaril HTML

1. Zapiši, kdo je avtor jezika HTML in kdaj je nastal.
2. Katera organizacija danes skrbi za standardizacijo jezika HTML?
3. V eni povedi razloži, kaj pomeni *W3C*.



Vaja 5: Prve različice HTML

1. Našteti so elementi, ki so bili uvedeni v različnih verzijah HTML. Označi, kateri so obstajali že v **HTML 1.0**:
   - tabele
   - naslovi
   - odstavki
   - seznami
   - povezave
   - obrazci
2. Katero novo možnost je prinesel **HTML5**?

Vaja 6: Hipertekst

1. V *Notepadu* ustvari nov dokument povezava.html.
2. Vpiši:

```
<p>Več informacij najdete na <a href="https://www.w3.org">spletnem
mestu W3C</a>.</p>
```

3. Shrani in odpri v brskalniku.
4. Klikni povezavo in opiši, kaj se zgodi.
5. Kako bi razložil pojem *hipertekst* s svojimi besedami?

Vaja 7: Kako deluje brskalnik?

1. V dokumentu index.html izbriši zaključni del </p> pri odstavku.
2. Shrani in odpri stran v brskalniku.
3. Kaj se zgodi? Ali brskalnik vseeno prikaže odstavek?
4. Zakaj pravi, da brskalnik "poskuša uganiti", kje se oznaka konča?

Vaja 8: HTML in informatika

1. Naštej tri primere, kako se HTML uporablja v organizacijah (v logistiki, podjetjih, javni upravi …).
2. Razloži, zakaj je **pravilna struktura HTML** pomembna za informacijsko varnost.
3. Kateri elementi lahko pomagajo zmanjšati napake pri objavi (npr. metapodatki, validacija)?

Vaja 9: Ustvari svoj prvi mini-splet

1. Ustvari mapo moj-projekt.
2. V njej datoteko index.html z osnovno strukturo HTML.
3. Dodaj naslov, dva odstavka in eno povezavo.
4. Shrani in preveri prikaz.
5. Poimenuj vsako oznako v datoteki in razloži, kaj dela.



Vaja 10: Preverjanje veljavnosti

1. Odpri https://validator.w3.org.
2. V polje **"*Validate by File Upload*"** naloži svoj index.html.
3. Preveri rezultat:
   - Če se pojavijo **napake**, jih zapiši in odpravi.
   - Če se pojavi **"*Document checking completed. No errors found.*"**, shrani dokazilo (posnetek zaslona).



Dodatna naloga

Razmisli, zakaj HTML sam po sebi ni "varen" jezik in zakaj pri razvoju spletnih strani potrebujemo tudi druge tehnologije (npr. CSS, *JavaScript*, HTTPS, varnostne politike).

Univerzitetna založba
Univerze v Mariboru

4 Osnovne HTML oznake za besedilo – naslovi, odstavki, povezave in slike

4.1 Uvod

Ko poznamo osnovno zgradbo dokumenta HTML (glavo in telo), lahko začnemo ustvarjati **vsebino**, ki jo vidi uporabnik.

Vsebino opisujemo z **oznakami (elementi)**, ki imajo določen pomen in funkcijo.

Najpogosteje uporabljeni osnovni elementi so:

- naslovi (<h1> … <h6>)
- odstavki (<p>)
- povezave (<a>)
- slike (<img>)

4.2 Naslovi

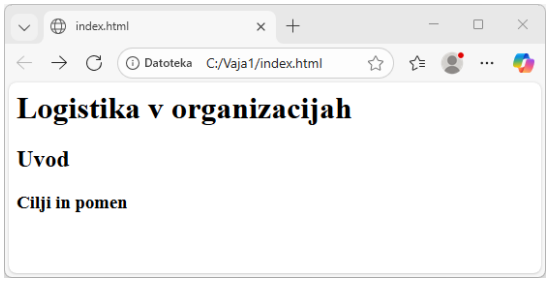
Naslovi so kot poglavja v knjigi – pomagajo urejati vsebino in jo narediti pregledno.

Tabela 35

Oznaka	Namen	Primer prikaza
<h1>	glavni naslov strani (pojavi se le enkrat)	velik in poudarjen
<h2>	naslov poglavja	manjši
<h3>–<h6>	podnaslovi	še manjši

Primer:

```
<h1>Logistika v organizacijah</h1>
<h2>Uvod</h2>
<h3>Cilji in pomen</h3>
```



Pravila:

- Hierarhija naj bo logična (h1 → h2 → h3 …).
- Ne preskakuj nivojev (npr. iz h1 takoj na h4).
- Naslovi pomagajo tudi **bralnikom zaslona**, zato vplivajo na **dostopnost**.

4.3 Odstavki

Element (angl. *paragraph*) označuje **odstavek besedila**.

Primer:

```
<p>Logistika je proces načrtovanja, izvajanja in nadzora pretoka
blaga, informacij in virov od izvora do porabe.</p>
```

Vsak odstavek naj bo v svoji oznaki ... .

Če želiš novo vrstico znotraj istega odstavka, lahko uporabiš oznako
 (angl. *break*).

Primer:

```
<p>To je prvi stavek.<br>To je drugi stavek v naslednji vrstici.</p>
```

Odstavki

Tabela 36

Oznaka	Učinek
 	Prelom vrstice znotraj istega odstavka.
<p>	Nov odstavek (večja navpična razdalja).
	Brez preloma – logično ločilo v isti vrstici.
	Nov blok (kot novi odstavek).

4.4 Povezave

Povezave so bistvo spleta — omogočajo premikanje med stranmi in dokumenti.

Uporabljamo oznako <a> (angl. *anchor*).

Osnovna oblika:

```
<a href="https://www.um.si">Univerza v Mariboru</a>
```

Atribut href (angl. *hyperlink reference*) določa **naslov (URL)**, kam vodi povezava.
Primeri:

```
<!-- Zunanja povezava -->
<a href="https://www.gov.si">Spletna stran Vlade RS</a>

<!-- Notranja povezava -->
<a href="kontakt.html">Kontakt</a>
```

Če želimo, da se zunanja povezava odpre v novem zavihku:

```
<a href="https://www.um.si" target="_blank" rel="noopener
noreferrer">Obišči UM</a>
```

Zakaj rel="noopener noreferrer"?

To pove brskalniku, da naj ne deli informacij o strani, iz katere prihajamo, kar povečuje **varnost in zasebnost**.

4.5 Slike

Z oznako <img> vstavljamo slike.

Ta oznaka **nima zaključne oznake** in zahteva vsaj dva atributa:

Tabela 37

Atribut	Pomen
src	pot do slike (datoteka ali URL)
alt	alternativno besedilo, če slike ni mogoče prikazati

Primer:

```
<img src="slika.jpg" alt="Tovornjak na cesti">
```

Pravila:

- Slike vedno shrani v podmapo, npr. images/.
- Uporabi kratke in jasne opise v alt – pomembno za dostopnost.
- Če je slika dekorativna, lahko uporabiš alt="".
- Za hitrejše nalaganje uporabljaj manjše slike (.jpg, .webp).

Primer s podmapo:

```
<img src="images/vozilo.jpg" alt="Vozilo v skladišču">
```

4.6 Absolutne in relativne poti pri povezavah

Preden začnemo ustvarjati povezave med spletnimi stranmi, moramo razumeti, kako določimo **pot do datoteke**, na katero jih želimo povezati. Pri tem uporabljamo **absolutne** ali **relativne** poti.

Pravilno razumevanje poti je temelj za medsebojno povezovanje več html dokumentov.

4.6.1 Absolutne poti

Absolutna pot vsebuje popoln naslov do datoteke ali spletne strani.

Vedno se nanaša na isto lokacijo, ne glede na to, od kod dostopamo.

Uporabljamo jo predvsem za povezave na **zunanje spletne strani**.

Primeri absolutnih poti:

Spletni naslov (URL):

```
<a href="https://www.um.si">Univerza v Mariboru</a>
```

Lokalna pot (manj pogosto v praksi):

```
<a href="C:/Users/Miha/Documents/projekt/index.html">Lokalna
datoteka</a>
```

Kdaj uporabljamo absolutno pot?

- Kadar povezujemo na spletne strani izven našega projekta,
- kadar želimo, da povezava deluje enako na vseh napravah in lokacijah.

4.6.2 Relativna pot

Relativna pot opisuje lokacijo datoteke **glede na datoteko, v kateri se trenutno nahajamo**.

Uporabljamo jo pri povezovanju **podstrani znotraj iste mape oziroma projekta**.

Primeri relativnih poti:

Datoteka je v isti mapi:

```
<a href="onas.html">O nas</a>
```

Datoteka v podmapi:

```
<a href="podatki/porocilo.html">Poglej poročilo</a>
```

Datoteka v nadrejeni mapi:

```
<a href="../index.html">Nazaj na domov</a>
```

Zakaj uporabljamo relativne poti?

- Delujejo tudi, če projekt premaknemo na USB ali drug računalnik,
- so preglednejše in krajše,
- so priporočene pri spletnih projektih.

4.6.3 Simboli pri relativnih poteh

Pri relativnem naslavljanju lahko uporabljamo posebne oznake:

Tabela 38

Zapis	Pomen	Razlaga
./	trenutna mapa	"tu, kjer sem zdaj"
../	nadrejena mapa	"pojdi eno mapo višje"
../../	dve ravni višje	"pojdi dve mapi višje"

Primer strukture map:

```
projekt/
├─ Q/
│  └─ podatki1.html
└─ R/
   └─ S/
      └─ podatki2.html   ← tukaj se nahajamo
```

Povezava iz podatki2.html na podatki1.html:

```
<a href="../../Q/podatki1.html">Na podatki1</a>
```

Enakovredno in jasnejše (obdrži ./):

```
<a href="./../../Q/podatki1.html">Na podatki1</a>
```

Obe varianti sta pravilni. Druga je didaktično preglednejša, saj izrecno pokaže, da izhajamo iz trenutne mape.

4.6.4 Pogoste napake pri uporabi poti

- **Uporaba \ namesto /**
  Pot mora **vedno** vsebovati **poševnice naprej** /.

- **Začetni / pri lokalnih datotekah**
  Zapis, ki se začne z /, brskalnik razume kot **koren spletnega strežnika**, ne kot lokalno mapo projekta.
- **Neupoštevanje izhodiščne datoteke**
  Pogosta napaka je, da pot računamo glede na index.html.
  Relativna pot se vedno nanaša na datoteko, v kateri se trenutno nahajamo.

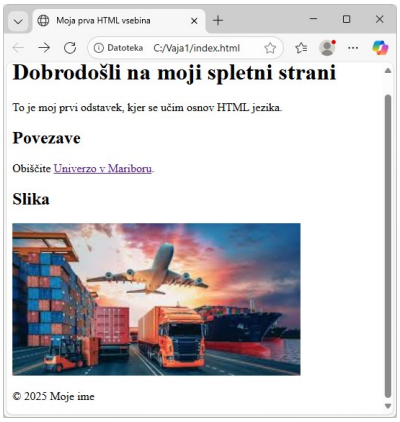
Kratek povzetek

Tabela 39

Vrsta poti	Primer	Kdaj jo uporabimo
Absolutna	https://www.um.si/info.html	Ko povezujemo na zunanje strani.
Relativna	../kontakt.html	Ko povezujemo notranje podstrani v projektu.

4.7 Praktičen primer

Ustvari datoteko index.html z naslednjo vsebino:




```
<!DOCTYPE html>
<html lang="sl">
<head>
  <meta charset="UTF-8">
  <title>Moja prva HTML vsebina</title>
</head>
<body>
  <h1>Dobrodošli na moji spletni strani</h1>
  <p>To je moj prvi odstavek, kjer se učim osnov HTML jezika.</p>

  <h2>Povezave</h2>
  <p>Obiščite <a href="https://www.um.si" target="_blank"
rel="noopener noreferrer">Univerzo v Mariboru</a>.</p>

  <h2>Slika</h2>
  <img src="images/logistika.jpg" alt="Logistični center"
width="400">

  <p>&copy; 2025 Moje ime</p>
</body>
</html>
```

4.8 Samostojna naloga

1. V *Notepadu* ustvari novo mapo html-vaje.
2. Vanjo shrani datoteko index.html.
3. Dodaj:
   - en glavni naslov (h1),
   - dva podnaslova (h2),
   - dva odstavka (p),
   - eno zunanjo povezavo (a),
   - eno sliko (img).
4. Odpri datoteko v brskalniku in preveri, ali deluje.
5. (Dodatno) Preveri datoteko v HTML Validatorju.

4.9 Povzetek

Tabela 40

Element	Namen	Primer
<h1>–<h6>	naslovi	Podpoglavje
	odstavek	Besedilo...
<a>	povezava	Klikni
<img>	slika	<img src=\"slika.jpg\" alt=\"Opis\">

4.10 Vaje za poglavje 4 – Osnovne HTML oznake za besedilo: naslovi, odstavki, povezave in slike

Vaja 1: Prepoznaj elemente

1. Odpri datoteko index.html, ki si jo ustvaril pri prejšnjih vajah.
2. Preštej, kolikokrat se pojavi oznaka <h1>, in <a>.
3. Zapiši, kateri deli strani so vidni in kateri niso (npr. <title> se prikaže v zavihku).

Vaja 2: Hierarhija naslovov

1. V *Notepadu* ustvari nov dokument naslovi.html.
2. Vpiši primere naslovov od <h1> do <h6>.
3. Odpri v brskalniku in opazuj velikost posameznih naslovov.
4. Dopolni z odgovorom: Zakaj je priporočljivo uporabiti samo en <h1> na stran?



Vaja 3: Logična struktura besedila

1. V dokumentu naslovi.html dodaj tri odstavke (<p>), ki opisujejo temo tvoje izbire (npr. logistika, varnost, šport).
2. Med vsakim odstavkom vstavi prelom vrstice <br>.
3. Preveri prikaz v brskalniku.
4. Razloži, kdaj uporabimo <br> in kdaj nov <p>.



Vaja 4: Povezave na zunanje strani

1. Ustvari novo datoteko povezave.html.
2. Vpiši:

```
<a href="https://www.um.si">Univerza v Mariboru</a>
```

3. Odpri datoteko v brskalniku in klikni povezavo.
4. Dodaj še eno povezavo na spletno mesto https://www.gov.si.
5. Preveri, kako se povezava obnaša, če dodaš atribut target="_blank".



Vaja 5: Povezave med lokalnimi stranmi

1. V mapi html-vaje ustvari tri datoteke:

   index.html, onas.html, kontakt.html.

2. V index.html dodaj povezave do drugih dveh datotek:

```
<a href="onas.html">O nas</a> | <a href="kontakt.html">Kontakt</a>
```

3. V vsako podstran dodaj povezavo “Nazaj na domov”.
4. Preveri, da vse povezave delujejo pravilno.



Vaja 6: Varne povezave

1. V dokumentu povezave.html spremeni vse zunanje povezave, da se odprejo v novem zavihku:

```
<a href="https://www.um.si" target="_blank" rel="noopener noreferrer">
```

2. Razloži v dveh stavkih, zakaj uporabljamo rel="noopener noreferrer".
3. Preveri delovanje v brskalniku.



Vaja 7: Slika na spletni strani

1. V mapi html-vaje ustvari podmapo images.
2. Vanjo shrani eno sliko (npr. slika.jpg).
3. V datoteko index.html dodaj vrstico:

```
<img src="images/slika.jpg" alt="Primer slike" width="400">
```

4. Odpri stran in preveri, ali se slika prikaže.
5. Poskusi odstraniti atribut alt — kaj se zgodi, če sliko preimenuješ ali izbrišeš?



Vaja 8: Preveri dostopnost slik

1. Odpri svoj dokument index.html.
2. Preveri, ali ima vsaka slika opisni atribut alt.
3. Zapiši, zakaj je ta atribut pomemben za:
   - uporabnike s slabovidnostjo,
   - počasne internetne povezave,
   - iskalnike.



Vaja 9: Kombinacija vseh osnovnih oznak

1. V *Notepadu* ustvari nov dokument vsebina.html.
2. Dodaj:
   - glavni naslov (<h1>),
   - dva podnaslova (<h2>),
   - tri odstavke (<p>),
   - eno zunanjo povezavo (<a>),
   - eno sliko (<img>).
3. Shrani in preveri prikaz v brskalniku.
4. Preveri veljavnost na https://validator.w3.org.

Vaja 10: Samostojna mini-stran

1. Združi znanje iz vseh prejšnjih vaj.
2. Ustvari mapo mini-projekt.
3. Vanjo shrani tri datoteke:
   - index.html – glavni naslov in opis,
   - povezave.html – seznam povezav,
   - slike.html – prikaz dveh slik z opisi.
4. Vse poveži med seboj s povezavami.
5. Dodaj svoje ime in letnico v nogo strani.
6. Preveri pravilnost delovanja v brskalniku.

Vaja: Absolutne poti

Namen: Razumeti, kdaj uporabljamo absolutne poti in kako delujejo neodvisno od lokacije datoteke.

1. Ustvari novo datoteko **povezave-absolutne.html** v mapi *html-vaje*.
2. Dodaj tri povezave, ki uporabljajo **absolutne poti**:
   - Povezava na spletno stran tvoje fakultete,
   - Povezava na spletno stran vlade,
   - Povezava na poljubno zunanjo stran po tvoji izbiri.

Primer:

```
<a href="https://www.um.si">Univerza v Mariboru</a>
<br>
<a href="https://www.gov.si">Vlada RS</a>
<br>
<a href="https://www.google.com">Google</a>
```

3. Shrani datoteko in jo odpri v brskalniku. Klikni vse tri povezave.

4. **Vprašanja za razmislek:**
   a) Zakaj te povezave delujejo, tudi če datoteko premakneš na USB, drug računalnik ali v drugo mapo?

b) Kdaj je smiselno uporabiti absolutno pot namesto relativne? Navedi vsaj dva primera.



Vaja: Relativne poti

Namen: Razumeti, kako pravilno uporabljamo relativne poti med datotekami znotraj istega projekta.

1. Ustvari novo mapo **moj-splet** in v njej naslednjo strukturo:

```
moj-splet/
│
├─ index.html
├─ o-nas.html
└─ info/
   ├─ kontakt.html
   └─ galerija.html
```

2. V datoteko **index.html** dodaj povezave do obeh podstrani v mapi *info*:

```
<a href="info/kontakt.html">Kontakt</a> |
<a href="info/galerija.html">Galerija</a>
```

3. V datoteko **kontakt.html** dodaj povezavo **nazaj na index.html** z uporabo relativne poti:

```
<a href="../index.html">Nazaj na domov</a>
```

4. V datoteko **o-nas.html** dodaj povezavo do galerije:

```
<a href="info/galerija.html">Galerija</a>
```

5. **Izvedi test:**
   a) Odpri index.html in klikaj vse povezave – ali delujejo pravilno?
   b) Nato **premakni celotno mapo** moj-splet na namizje ali USB. Preveri, ali povezave še vedno delujejo.
6. **Naloga za razmislek:**
   a) Kaj bi se zgodilo, če namesto ../index.html v *kontakt.html* uporabiš absolutno pot?
   b) V kateri situaciji je relativna pot boljša od absolutne?



Projektna vaja: Absolutne in relativne poti v praksi

Namen: Študent izdela mini spletno stran z več podstranmi, pri čemer mora smiselno uporabiti **absolutne** in **relativne** poti.

Cilj: Ustvari delujoč spletni projekt, ki vsebuje vsaj 4 HTML datoteke, pravilno strukturo map ter različne vrste povezav.

Načrt

Najprej si na list papirja *nariši* ali v zvezek zapiši predlagano strukturo map.

Projekt naj ima naslednjo strukturo (lahko jo po želji razširiš):

```
moja-stran/
│
├─ index.html
├─ o-meni.html
├─ povezave.html
└─ materiali/
   ├─ slike.html
   └─ dokumenti/
      └─ info.html
```

- *index.html* – glavna stran
- *o-meni.html* – osebna predstavitev
- *povezave.html* – vsebuje vsaj 3 **absolutne povezave**
- *materiali/slike.html* – vsebuje slike (lahko tudi prazne slike)
- *materiali/dokumenti/info.html* – informativna podstran

Naloga

Ustvari zgornjo strukturo map. Nato v vsako stran dodaj povezave:

- **A. Uporabi ABSOLUTNE poti**

V datoteki **povezave.html** dodaj vsaj tri zunanje povezave:

- tvoja fakulteta ali šola,

- stran Vlade RS,
- ena poljubna spletna stran.

Primer:

```
<a href="https://www.um.si" target="_blank">Univerza v Mariboru</a>
```

– B. Uporabi RELATIVNE poti

1. V **index.html** dodaj povezave na vse ostale podstrani:

```
<a href="o-meni.html">O meni</a> |
<a href="povezave.html">Povezave</a> |
<a href="materiali/slike.html">Slike</a>
```

2. V **slike.html** dodaj povezavo nazaj na glavno stran:

```
<a href="../index.html">Nazaj na domov</a>
```

3. V **info.html** dodaj dve povezavi:
   - eno v *slike.html* (relativno pot),
   - eno v *index.html* (relativno pot prek dveh map).

Primer:

```
<a href="../slike.html">Slike</a>
<a href="../../index.html">Domov</a>
```

Test delovanja

Ko končaš:

1. Odpri **index.html** v brskalniku.
2. Preveri, ali lahko prideš do vseh:
   notranjih strani z relativnimi potmi
   zunanjih strani z absolutnimi potmi
3. Premakni celotno mapo *moja-stran* na USB ali namizje.
   → Preveri, ali **relativne povezave še vedno delujejo**.

Refleksija (zapiši odgovore)

Na konec v datoteko **povezave.html** dodaj komentar (HTML komentar <!-- ... -->) z odgovori:

```
<!--
Kaj sem se naučil/a o absolutnih poteh?
Kdaj so relativne poti boljše od absolutnih?
Katero napako sem pri povezavah sprva naredil/a?
-->
```

Dodatno

Razširi projekt z vsaj eno od možnosti:

- dodaj mapo *assets* s slikami in jih pravilno poveži
- dodaj datoteko *viri.html* z zunanjimi povezavami (absolutne poti)
- ustvari navigacijski meni na vsaki strani



Dodatna naloga

V index.html dodaj znak za avtorske pravice © in poseben znak €.

Razloži, zakaj HTML uporablja posebne entitete za prikaz določenih znakov.

Univerzitetna založba
Univerze v Mariboru

5 Struktura spletne strani – uporaba seznamov, tabel in razdelkov (header, nav, main, footer)

5.1 Uvod

Ko znamo ustvariti osnovne HTML elemente (naslove, odstavke, povezave in slike), sledi naslednji korak — **urediti vsebino v logično strukturo**.

To pomeni, da spletna stran ni le zaporedje besedila, ampak ima **semantične dele**, ki brskalniku in uporabniku povedo, kaj posamezni del pomeni.

5.2 Kaj pomeni semantična struktura?

Semantični elementi so tisti, ki imajo svoj pomen (semantiko).

Namesto da uporabimo zgolj za vse dele, uporabimo bolj natančne oznake, kot so:

Tabela 41

Element	Namen
<header>	glava strani ali poglavja (naslov, logotip, uvodni del)
<nav>	navigacija ali meni povezav
<main>	glavni vsebinski del
<section>	logičen razdelek vsebine
<article>	samostojna vsebinska enota (npr. novica, objava)
<aside>	dodatne informacije, stranska vsebina
<footer>	noga strani (avtor, kontakt, datum, licence …)

Ti elementi pomagajo pri:

- **dostopnosti** (bralniki zaslona lažje razumejo strukturo),
- **optimizaciji za iskalnike (*SEO*)**,
- **urejenosti kode**.

5.3 Osnovna postavitev strani

Spodaj je primer celotne osnovne strukture spletne strani z uporabo semantičnih elementov:

```
<!DOCTYPE html>
<html lang="sl">
<head>
  <meta charset="UTF-8">
  <title>Primer spletne strani</title>
</head>
<body>

  <header>
    <h1>Informatika in informacijska varnost</h1>
    <p>Fakulteta za logistiko – Univerza v Mariboru</p>
  </header>

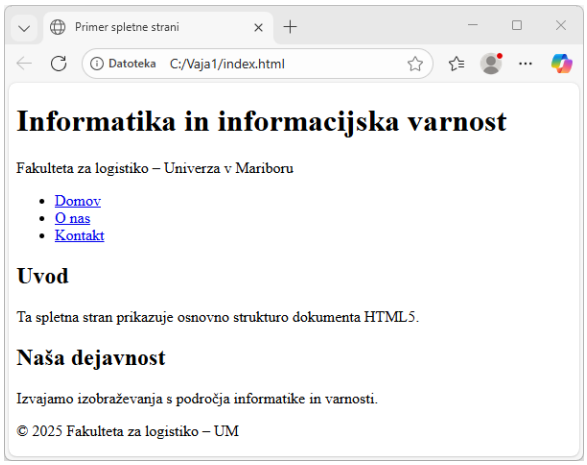
  <nav>
    <ul>
      <li><a href="index.html">Domov</a></li>
      <li><a href="onas.html">O nas</a></li>
      <li><a href="kontakt.html">Kontakt</a></li>
    </ul>
  </nav>
```

```
  <main>
    <section>
      <h2>Uvod</h2>
      <p>Ta spletna stran prikazuje osnovno strukturo dokumenta
HTML5.</p>
    </section>

    <section>
      <h2>Naša dejavnost</h2>
      <p>Izvajamo izobraževanja s področja informatike in
varnosti.</p>
    </section>
  </main>

  <footer>
    <p>&copy; 2025 Fakulteta za logistiko – UM</p>
  </footer>

</body>
</html>
```

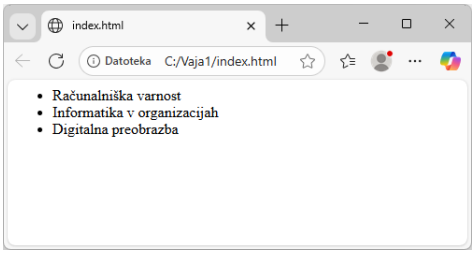


5.4 Uporaba seznamov

Seznami omogočajo urejen prikaz informacij ali povezav.

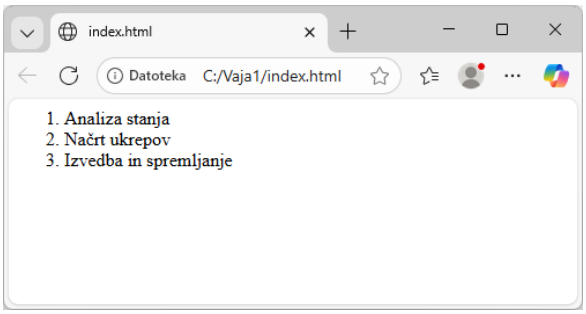
5.4.1 Neurejen seznam (oznaka s pikami)

```
<ul>
  <li>Računalniška varnost</li>
  <li>Informatika v organizacijah</li>
  <li>Digitalna preobrazba</li>
</ul>
```



5.4.2 Urejen seznam (številke)

```
<ol>
  <li>Analiza stanja</li>
  <li>Načrt ukrepov</li>
  <li>Izvedba in spremljanje</li>
</ol>
```



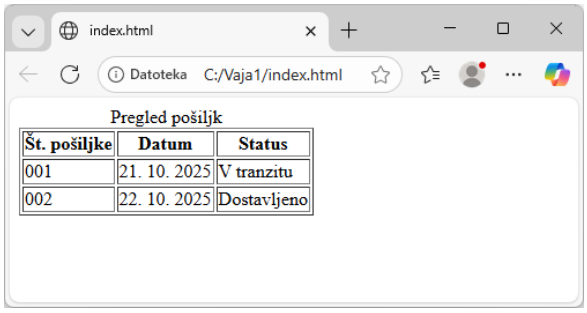
Sezname pogosto uporabimo tudi za **navigacijske menije**, saj <li> elementi lepo urejajo povezave.

5.5 Tabele

Tabele uporabljamo za **prikaz podatkov v mreži** (npr. seznam pošiljk, urnik, pregled zalog).

Primer:

```
<table border="1">
  <caption>Pregled pošiljk</caption>
  <tr>
    <th>Št. pošiljke</th>
    <th>Datum</th>
    <th>Status</th>
  </tr>
  <tr>
    <td>001</td>
    <td>21. 10. 2025</td>
    <td>V tranzitu</td>
  </tr>
  <tr>
    <td>002</td>
    <td>22. 10. 2025</td>
    <td>Dostavljeno</td>
  </tr>
</table>
```



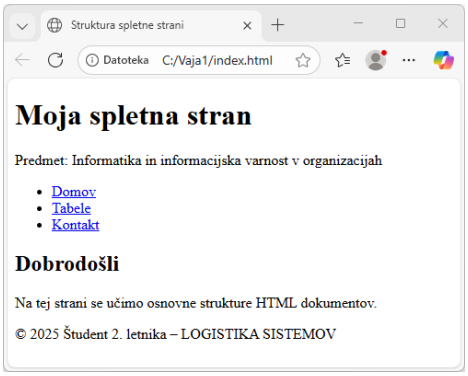
Pravila dobre prakse:

- <caption> dodamo kot naslov tabele.
- Glavo tabele postavimo v <th>, vrstice v <tr>, podatke v <td>.

– Čeprav atribut border še deluje, se v sodobnih straneh uporablja CSS, tukaj pa ga ohranimo zaradi enostavnosti.

Kako vse skupaj povežemo?

Ustvari mapo struktura/ in v njej datoteko index.html z naslednjo vsebino:




```
<!DOCTYPE html>
<html lang="sl">
<head>
  <meta charset="UTF-8">
  <title>Struktura spletne strani</title>
</head>
<body>

  <header>
    <h1>Moja spletna stran</h1>
    <p>Predmet: Informatika in informacijska varnost v
organizacijah</p>
  </header>

  <nav>
    <ul>
      <li><a href="index.html">Domov</a></li>
      <li><a href="tabela.html">Tabele</a></li>
      <li><a href="kontakt.html">Kontakt</a></li>
    </ul>
  </nav>

  <main>
    <section>
      <h2>Dobrodošli</h2>
      <p>Na tej strani se učimo osnovne strukture HTML dokumentov.</p>
    </section>
  </main>

  <footer>
    <p>&copy; 2025 Študent 2. letnika – LOGISTIKA SISTEMOV</p>
  </footer>

</body>
</html>
```

Nato ustvari še:

- **tabela.html** → vsebuje tabelo s pošiljkami (iz točke 5),
- **kontakt.html** → vsebuje kontaktne podatke in povezavo »Nazaj na domov«.

5.6 Naloga za samostojno delo

1. Ustvari tri datoteke: index.html, tabela.html, kontakt.html.
2. V index.html dodaj glavo, meni in glavni del s kratkim opisom.
3. V tabela.html prikaži tabelo (npr. pregled pošiljk).
4. V kontakt.html napiši svoj e-naslov in povezavo nazaj na index.html.
5. Preveri, da vse povezave delujejo pravilno.

5.7 Povzetek

Tabela 42

Element	Namen	Primer
`<header>`	glava strani	`<header><h1>Naslov</h1></header>`
`<nav>`	navigacija	`<nav><ul><li><a href=\"...\">Link</a></li></ul></nav>`
`<main>`	glavni vsebinski del	`<main><section>...</section></main>`
`<footer>`	noga strani	`<footer>Kontakt</footer>`
`<ul> / <ol>`	seznami	`<ul><li>1</li></ul>`
`<table>`	tabele	`<table><tr><th></th></tr></table>`

5.8 Vaje za poglavje 5 – Struktura spletne strani: seznami, tabele in razdelki



Vaja 1: Prepoznaj semantične elemente

1. Preglej spodnji seznam oznak: <header>, <nav>, <main>, <section>, <footer>, .
2. Označi, katere od njih so **semantične** (z določenim pomenom) in katere **ne**.
3. Zapiši, čemu služi vsak semantični element (npr. *header – glava strani*).



Vaja 2: Osnovna zgradba spletne strani

1. Odpri *Notepad* in ustvari nov dokument struktura.html.
2. Vpiši osnovno strukturo HTML5 (<!DOCTYPE html> …).
3. V <body> dodaj naslednje oznake: <header>, <nav>, <main>, <footer>.

4. V vsak del vpiši kratko besedilo (npr. “To je glava strani”).
5. Odpri v brskalniku in preveri, ali so vsi deli vidni.



Vaja 3: Dodajanje naslovov in odstavkov

1. V razdelek <header> dodaj glavni naslov (<h1>Moja spletna stran</h1>).
2. V <main> dodaj dva razdelka (<section>) z naslovoma (<h2>) in po enim odstavkom (<p>).
3. Shrani kot index.html in preveri prikaz v brskalniku.
4. Katere dele strani bi moral videti uporabnik?



Vaja 4: Navigacijski meni

1. V razdelek <nav> dodaj seznam povezav:

```
<ul>
  <li><a href="index.html">Domov</a></li>
  <li><a href="onas.html">O nas</a></li>
  <li><a href="kontakt.html">Kontakt</a></li>
</ul>
```

2. Shrani in preveri prikaz v brskalniku.
3. Kako bi opisal razliko med oznakama <ul> in ?



Vaja 5: Ustvari podstran “O nas”

1. Ustvari novo datoteko onas.html.
2. Dodaj osnovno strukturo z <header>, <nav>, <main>, <footer>.
3. V <main> vpiši kratek opis organizacije ali področja logistike.
4. Dodaj povezavo »Nazaj na domov«:

   Nazaj na domov

5. Preveri delovanje povezav.

Vaja 6: Seznami vsebin

1. V datoteki index.html dodaj pod naslov "Naše dejavnosti" naslednji **neurejen seznam**:

```
<ul>
  <li>Informatika v organizacijah</li>
  <li>Informacijska varnost</li>
  <li>Digitalna logistika</li>
</ul>
```

2. Nato dodaj **urejen seznam** treh korakov logističnega procesa.
3. Preveri razliko v prikazu.

Vaja 7: Tabela s podatki

1. Ustvari novo datoteko tabela.html.
2. Vpiši primer tabele s tremi stolpci (št. pošiljke, datum, status).

   Uporabi oznake <table>, <tr>, <th>, <td>.

3. Dodaj naslov tabele s <caption>Pregled pošiljk</caption>.
4. Shrani in preveri prikaz v brskalniku.
5. Kaj se zgodi, če izbrišeš eno oznako </tr>?

Vaja 8: Povezovanje strani

1. V index.html dodaj povezave do tabela.html in kontakt.html.
2. V tabela.html in kontakt.html dodaj povezavo »Nazaj na domov«.
3. Shrani in preveri delovanje navigacije med vsemi tremi stranmi.

Vaja 9: Dopolni nogo strani

1. V vseh treh datotekah (index.html, tabela.html, kontakt.html) dodaj v razdelek <footer> besedilo:

   © 2025 Študent 2. letnika – Logistika sistemov

2. Odpri vse tri strani v brskalniku in preveri, da se noga prikaže pravilno.
3. Zakaj je smiselno imeti nogo na vsaki strani?



Vaja 10: Samostojni mini-projekt

1. Ustvari mapo stran/.
2. Vanjo shrani tri datoteke: index.html, tabela.html, kontakt.html.
3. Vsaka stran mora imeti:
   - glavo (*header*) z naslovom,
   - navigacijo (nav),
   - glavni del (*main* z vsaj enim *section*),
   - nogo (*footer*).
4. Vključi seznam in tabelo.
5. Poveži strani med seboj.
6. Preveri delovanje v brskalniku in validiraj vsako datoteko na https://validator.w3.org.



Dodatna naloga

Razmisli, kako bi lahko v prihodnje ločil **vsebino** (HTML) in **oblikovanje** (CSS).

Zapiši, zakaj je ločevanje teh dveh vidikov pomembno pri razvoju večjih spletnih sistemov.

Univerzitetna založba
Univerze v Mariboru

6 Osnove obrazcev (forms) – vnos podatkov, oznake in osnovna validacija

6.1 Kaj je obrazec v HTML?

Obrazec (*form*) je del spletne strani, v katerem uporabnik **vnaša podatke** — na primer:

- svoje ime, e-poštni naslov, geslo,
- izbiro izdelka,
- sporočilo ali komentar.

Obrazci so temelj **interaktivnih spletnih strani**, saj omogočajo pošiljanje podatkov strežniku ali njihovo obdelavo (čeprav v našem primeru podatkov še ne pošiljamo nikamor).

6.2 Osnovna struktura obrazca

Vsak obrazec je zapisan z oznako <form> in ima lahko naslednje dele:

```
<form action="..." method="post">
  <!-- polja za vnos -->
</form>
```

Tabela 43

Atribut	Pomen
action	določa, kam se podatki pošljejo (npr. datoteka ali spletna storitev)
method	določa način pošiljanja (get ali post)

V naših vajah bomo za zdaj pustili action="#", kar pomeni, da se podatki ne pošiljajo nikamor.

6.3 Najpogostejša polja za vnos

Tabela 44

Element	Namen	Primer
`<input type="text">`	navadno besedilno polje	`<input type="text" name="ime">`
`<input type="email">`	e-poštni naslov	`<input type="email" name="mail">`
`<input type="password">`	geslo	`<input type="password" name="geslo">`
`<input type="number">`	številčna vrednost	`<input type="number" name="kolicina">`
`<textarea>`	večvrstično besedilo	`<textarea name="sporocilo"></textarea>`
`<select>`	spustni seznam	`<select><option>...</option></select>`
`<button>`	gumb	`<button type="submit">Pošlji</button>`

6.4 Oznake

Oznaka <label> pove, kateremu polju pripada opis.

S tem:

- omogočimo pravilno delovanje za bralnike zaslona (dostopnost),
- povečamo območje klika,
- ohranimo preglednost kode.

Primer:

```
<label for="ime">Vaše ime:</label>
<input id="ime" type="text" name="ime" required>
```

Atribut for se mora ujemati z id polja, ki ga opisuje.

6.5 Atributi za osnovno validacijo

Brez programiranja lahko že v HTML uvedemo osnovne **preveritve vnosov** (validacijo):

Tabela 45

Atribut	Pomen
required	polje je obvezno
min / max	omejitev vrednosti (pri številkah)
maxlength	največje število znakov
pattern	vzorec (npr. za geslo ali telefonsko številko)
placeholder	besedilo, ki se prikaže v praznem polju

Primer:

```
<input type="password" name="geslo" required minlength="8"
placeholder="Vsaj 8 znakov">
```

6.6 Primer preprostega obrazca

Ustvari novo datoteko kontakt.html v mapi z vajami in vpiši naslednje:

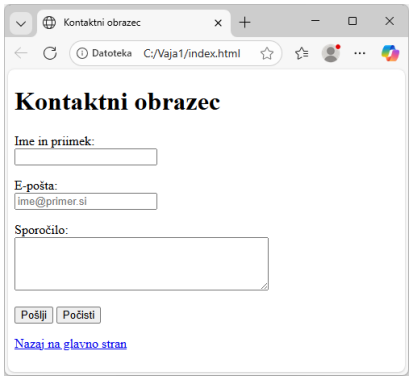
```
<!DOCTYPE html>
<html lang="sl">
<head>
  <meta charset="UTF-8">
  <title>Kontaktni obrazec</title>
</head>
<body>

  <h1>Kontaktni obrazec</h1>

  <form action="#" method="post">
    <p>
      <label for="ime">Ime in priimek:</label><br>
      <input type="text" id="ime" name="ime" required>
    </p>

    <p>
      <label for="email">E-pošta:</label><br>
      <input type="email" id="email" name="email"
placeholder="ime@primer.si" required>
    </p>

    <p>
      <label for="sporocilo">Sporočilo:</label><br>
      <textarea id="sporocilo" name="sporocilo" rows="4" cols="40"
maxlength="300"></textarea>
    </p>
```



```
      <p>
        <button type="submit">Pošlji</button>
        <button type="reset">Počisti</button>
      </p>
    </form>

    <p><a href="index.html">Nazaj na glavno stran</a></p>

  </body>
  </html>
```

Ko datoteko odpreš v brskalniku, lahko:

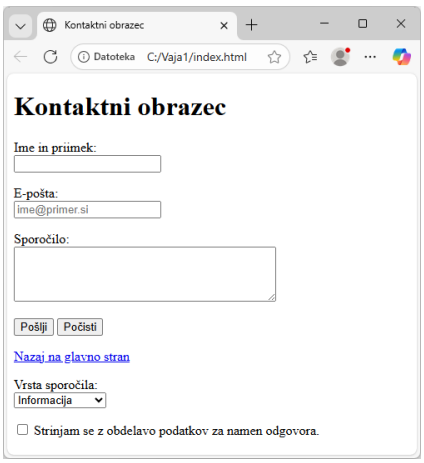
- izpolniš polja,
- vidiš opozorilo, če pustiš polje prazno,
- preizkusiš delovanje gumbov »Pošlji« in »Počisti«.

6.7 Primer: dodajanje dodatnih polj

Dodaj pod obrazec še **izbirna polja**:

```
<p>
  <label for="vrsta">Vrsta sporočila:</label><br>
  <select id="vrsta" name="vrsta">
    <option value="info">Informacija</option>
    <option value="povprasevanje">Povpraševanje</option>
    <option value="drugo">Drugo</option>
  </select>
</p>

<p>
  <input type="checkbox" id="strinjam" required>
  <label for="strinjam">Strinjam se z obdelavo podatkov za namen
odgovora.</label>
</p>
```



6.8 Kaj se zgodi, ko obrazec oddamo

V resničnih spletnih straneh se podatki iz obrazca pošljejo na **strežnik**, kjer jih obdela programska logika (npr. *PHP*, *Python*, ali *JavaScript*).

V tej fazi (osnove HTML) podatkov **ne pošiljamo**, ampak jih učimo:

- pravilne strukture,
- označevanja polj,
- osnovnega preverjanja vnosov.

6.9 Naloga za samostojno delo

1. Ustvari datoteko kontakt.html.
2. Dodaj polja: *ime*, *e-pošta*, *sporočilo* in *vrsta sporočila*.
3. Dodaj gumba "Pošlji" in "Počisti".
4. Preveri, da polja z *required* res zahtevajo vnos.
5. Dodaj povezavo "Nazaj na domov".
6. Shrani in preveri prikaz v brskalniku.

Povzetek

Tabela 46

Element	Namen	Primer
`<form>`	okvir obrazca	`<form action=\"#\" method=\"post\">...</form>`
`<input>`	vnosno polje	`<input type=\"text\" name=\"ime\">`
`<label>`	opis polja	`<label for=\"ime\">Ime:</label>`
`<textarea>`	večvrstično polje	`<textarea name=\"opis\"></textarea>`
`<select>`	spustni seznam	`<select><option>...</option></select>`
`<button>`	gumb	`<button type=\"submit\">Pošlji</button>`
`required, placeholder, pattern`	preverjanje vnosa	`<input required placeholder=\"...\">`

6.10 Vaje za poglavje 6 – Osnove obrazcev (forms)

Vaja 1: Prepoznaj obrazec

1. Odpri primer iz skripte in poišči oznako <form>.
2. Označi, kje se obrazec začne in kje konča.

3. Katere oznake so znotraj obrazca (npr. <input>, <label>, <button>)?
4. Zapiši, čemu služi *atribut method*.



Vaja 2: Ustvari preprost obrazec

1. Odpri *Notepad* in ustvari novo datoteko vnos.html.
2. Vpiši osnovno strukturo HTML in dodaj preprost obrazec:

```
<form action="#" method="post">
  <p><label for="ime">Ime:</label><br>
  <input type="text" id="ime" name="ime"></p>
</form>
```

3. Shrani in odpri v brskalniku.
4. Preveri, ali se polje za vnos prikaže.



Vaja 3: Dodaj več vnosnih polj

1. V obrazec dodaj naslednja polja:
   - e-poštni naslov (type="email"),
   - geslo (type="password"),
   - številko (type="number").
2. Odpri v brskalniku in preveri razliko med vrstami polj.
3. Kaj se zgodi, če v polje *email* vpišeš napačen format (npr. brez @)?



Vaja 4: Uporaba oznak <label>

1. Vsem poljem dodaj ustrezne oznake <label>.
2. Poskrbi, da se vrednosti for in id ujemajo (npr. for="geslo" in id="geslo").
3. Klikni na napis ob polju – ali se polje samodejno izbere?
4. Zakaj je to pomembno za dostopnost uporabnikov?



Vaja 5: Dodaj polje za sporočilo

1. Pod obstoječa polja dodaj:

```
<label for="sporocilo">Sporočilo:</label><br>
```

```
<textarea id="sporocilo" name="sporocilo" rows="4"
   cols="40"></textarea>
```

2. Preveri razliko med <textarea> in <input type="text">.
3. Dodaj atribut maxlength="300" in preveri, ali te omeji pri pisanju.



Vaja 6: Dodaj spustni seznam in potrditveno polje

1. V obrazec vključi:

```
<label for="vrsta">Vrsta sporočila:</label><br>
<select id="vrsta" name="vrsta">
  <option value="info">Informacija</option>
  <option value="povprasevanje">Povpraševanje</option>
  <option value="drugo">Drugo</option>
</select>
```

2. Dodaj potrditveno polje:

```
<input type="checkbox" id="strinjam" required>
<label for="strinjam">Strinjam se z obdelavo podatkov.</label>
```

3. Kaj se zgodi, če klikneš gumb *Pošlji* brez potrditve?



Vaja 7: Dodaj gumbe

1. Na konec obrazca dodaj gumba:

```
<button type="submit">Pošlji</button>
<button type="reset">Počisti</button>
```

2. Preveri razliko med obema gumboma.
3. Kaj se zgodi s polji, ko klikneš *Počisti*?



Vaja 8: Preverjanje z atributi

1. Dodaj naslednje zahteve:
   - Polje *ime* naj bo **obvezno** (required).
   - Geslo naj ima **najmanj 8 znakov** (minlength="8").

   - E-pošta naj ima **placeholder** "ime@primer.si".
2. Preveri v brskalniku, ali se pojavi opozorilo pri praznih ali napačnih vnosih.
3. Zapiši, katero preverjanje izvaja že brskalnik, brez dodatne kode.



Vaja 9: Celoten kontaktni obrazec

1. Ustvari datoteko kontakt.html.
2. Dodaj glavni naslov (<h1>Kontaktni obrazec).
3. Vključi vse elemente:
   - Ime in priimek,
   - E-poštni naslov,
   - Sporočilo,
   - Vrsta sporočila (spustni seznam),
   - Potrditveno polje,
   - Gumba *Pošlji* in *Počisti*.
4. Dodaj povezavo "Nazaj na glavno stran".
5. Preveri delovanje v brskalniku.



Vaja 10: Preverjanje in razmislek

1. Naloži datoteko kontakt.html na https://validator.w3.org.
2. Odpravi morebitne napake.
3. Razmisli in zapiši:
   - Zakaj je preverjanje (validacija) pomembno?
   - Kakšna so tveganja, če spletna stran sprejema vnose brez preverjanja?



Dodatna naloga

Razširi svoj obrazec tako, da uporabnik lahko izbere tudi **datum** (z <input type="date">) in naloži **datoteko** (z <input type="file">).

Razloži, zakaj je treba pri takšnih poljih paziti na **varnost** in **pravila zasebnosti**.

Univerzitetna založba
Univerze v Mariboru

7 Razvoj HTML

Pregled različic povzemamo po NSA (2025) in uradnih specifikacijah.

– HTML 1.0 (1990–1993)

Avtor: Tim Berners-Lee (CERN)
Opis: Prva različica jezika za opis hiperpovezanih dokumentov. Podpirala je osnovne elemente (naslovi, odstavki, povezave, sezname).
Brskalnik: *Mosaic* (1993, NCSA) – prvi javno dostopen brskalnik.
Opombe: HTML 1.0 ni bil formalno standardiziran, vendar je postavil temelje svetovnega spleta.

– HTML 2.0 (1995)

Standard: RFC 1866 – *IETF Recommendation*, 22. 9. 1995 (Berners-Lee in Connolly, 1995)
Opis: Prva uradna standardizacija jezika HTML. Vključuje obrazce, povezave, naslove, sezname, citate in osnovno strukturo strani.
Pomen: Postal je osnovni standard do leta 1997.

– HTML 3.0 (1995–1996)

Avtor: Dave Raggett (IETF)
Opis: Predlagal napredne funkcije – matematični zapisi, tabele, večslojni prikaz, slogovne razširitve.
Težave: Brskalniki niso bili dovolj zmogljivi, zato se standard ni uveljavil.
Status: *HTML 3.0 Specification, 28. 9. 1995 (Internet Draft)* – nikoli uradno sprejet.

– HTML 3.2 (1997)

Standard: *W3C Recommendation*, 14. 1. 1997 (Raggett, 1997)
Opis: Prva verzija, ki jo je standardiziral *W3C*.
Novosti: Tabele, skripti (*JavaScript*), matematični simboli, slogovne oznake (<font>,).
Pomen: Vzpostavila enotnost med brskalniki po t. i. "vojni brskalnikov" (*Netscape* vs. *Microsoft*).

– HTML 4.0 (1997–1998)

Standard:

- *W3C Proposed* Recommendation, 7. 11. 1997
- *W3C Recommendation*, 18. 12. 1997
- Popravki: 24. 4. 1998

Novosti:

- Podpora za **CSS** (*Cascading Style Sheets*)
- Internacionalizacija (*Unicode*, jeziki)
- Struktura dokumenta z elementi in
- Obrazci in skripti

Pomen: Ločitev med vsebino in oblikovanjem.

– HTML 4.01 (1999)

Standard: W3C Recommendation, 24. 12. 1999 (Raggett idr., 1999)
Opis: Popravki in dopolnitve različice 4.0.
Različice: Strict, Transitional in Frameset DTD.
Pomen: Dolgo časa najširše uporabljena različica.

– XHTML 1.0 (2000–2002)

Standard: *W3C Recommendation*, 26. 1. 2000 → 1. 8. 2002 (Pemberton idr., 2002)
Opis: HTML prepisan po pravilih *XML*.

Novosti: Strožja sintaksa (vse oznake morajo biti zaprte, pravilno gnezdene).
Pomen: Združitev HTML in XML logike; brez novih funkcionalnosti.

– XHTML 1.1 (2001–2007)

Standard: *W3C Recommendation*, 31. 5. 2001 (McCarron in Ishikawa, 2010)
Opis: Modularna zasnova jezika XHTML, razširjena za mobilne naprave in ločene profile.
Pomen: Poskus poenotenja različnih naprav – omejen uspeh.

– XHTML 2.0 (2002–2010)

Status: Nikoli sprejet (*W3C Working Draft*, 5. 8. 2002 – 16. 12. 2010)
Opis: Ambiciozen projekt za popolno prenovo HTML, a nezdružljiv s prejšnjimi različicami.
Rezultat: Projekt opuščen leta 2010 v korist HTML5.

– HTML 5 (2008–2014)

Standard:

- *W3C Working Draft*, 22. 1. 2008
- *W3C Candidate Recommendation*, 17. 12. 2012
- *W3C Recommendation*, 28. 10. 2014

Novosti:

- Novi semantični elementi: <header>, <footer>, <section>, <article>
- Multimedijski elementi: <video>, <audio>
- 2D grafika z <canvas>
- Lokalno shranjevanje (*Web Storage*)
- *Drag-and-drop*, geolokacija, SVG in *MathML* podpora

Pomen: Prelomna točka – HTML postane bogata spletna platforma.

– HTML 5.1 (2016)

Standard: *W3C Recommendation*, 1. 11. 2016
Opis: Posodobitev z izboljšanimi API-ji, dodatnimi atributi in poenotenimi elementi.

– HTML 5.2 (2017)

Standard: *W3C Recommendation*, 14. 12. 2017
Opis: Odprava nezdružljivosti, izboljšana dostopnost (*accessibility*), nove spletne funkcije.

– HTML 5.3 (2017–2018)

Status: W3C Working Draft
Opis: Pripravljalni korak k modelu "*Living Standard*".
Opombe: Nikoli ni postal končni standard, saj se je razvoj preselil k *WHATWG*.

– HTML – Living Standard (2019–danes)

Izdajatelj: *WHATWG* - https://html.spec.whatwg.org/multipage/ (Web Hypertext Application Technology Working Group, 2025)

Prenos pristojnosti: 28. 5. 2019 – *W3C* preda razvoj *WHATWG*.

Opis:

- HTML postane »živi standard« (stalno posodabljan brez verzij).
- Enotna, ažurna specifikacija za vse brskalnike.
- Vključuje definicije *DOM, API, JavaScript* integracije in dostopnosti.

Pomen: Današnji HTML ni več "verzija 6", ampak kontinuiran razvoj *HTML Living Standard*.

Povzetek razvoja HTML

Tabela 47

Obdobje	Organizacija	Verzije	Standardi / RFC
1990–1995	CERN / IETF	HTML 1.0, 2.0	RFC 1866
1996–2000	W3C	HTML 3.2, 4.0, 4.01	W3C Recs
2000–2010	W3C	XHTML 1.x, XHTML 2.0	RFC 3236, W3C Recs
2008–2017	W3C / WHATWG	HTML5, 5.1, 5.2	RFC 8081, W3C Recs
2019–danes	WHATWG	HTML Living Standard	Online “Living Standard”

Univerzitetna založba
Univerze v Mariboru

8 Sklep

V tem sklopu smo spoznali HTML kot temeljni gradnik spleta. Za vsako spletno stranjo, ki jo brskalnik prikaže v delčku sekunde, stoji preprosto berljiv dokument iz oznak in vsebine, ki ga zna prebrati vsak računalnik na svetu. Prav ta preprostost je razlog, da se je jezik iz skromne zamisli Tima Bernersa-Leeja razvil v standard, na katerem danes temelji celotno svetovno spletišče.

Naučili smo se, da HTML ni programski jezik, temveč označevalni jezik. Ne vsebuje logike, ampak vsebini pripisuje pomen in strukturo. Ta na videz drobna razlika nosi pomembno sporočilo. Vsebina in njen pomen sta ločena od videza, zato isto stran enako dobro razumejo brskalnik na telefonu, iskalnik in bralnik zaslona.

Spoznali smo zgradbo dokumenta z glavo in telesom, osnovne oznake za naslove, odstavke, povezave in slike, absolutne in relativne poti, semantične razdelke za glavo, navigacijo, osrednjo vsebino in nogo strani ter sezname, tabele in obrazce. Vsak od teh gradnikov rešuje svoje vprašanje, skupaj pa omogočajo, da iz golega besedila nastane urejena, povezana in uporabna spletna stran z več podstranmi.

Pomembno spoznanje sklopa je, da za delo s spletnimi tehnologijami ne potrebujemo dragih orodij.

Preprost urejevalnik besedila, brskalnik in spletni validator W3C zadoščajo, da stran zgradimo, preverimo njeno veljavnost in jo postopoma izboljšujemo. Potrebna pa sta natančnost in doslednost, saj brskalnik napako sicer pogosto skrije, a rezultat ni nujno tak, kot smo ga želeli.

Tudi pri HTML se tehnično znanje prepleta z varnostnim. Kdor pozna zgradbo spletne strani, zna presoditi, katere podatke je varno objaviti, poskrbi za dostopnost z opisi slik, preveri, kam vodijo povezave, in hitreje prepozna ponarejeno stran ali obrazec, ki krade podatke. Obrazci so nas poleg tega naučili, da je treba vsak vnos uporabnika preveriti, kar je prvo načelo varnega razvoja spletnih rešitev.

Za strokovnjaka s področja logistike to niso obrobne veščine. Spletni portali za naročanje in sledenje pošiljkam, obrazci za stranke in samodejno ustvarjena sporočila so vsakdanja orodja oskrbovalnih verig. Kdor razume, kako so zgrajena, lažje sodeluje pri njihovem naročanju in prenovi, presodi njihovo kakovost in prepozna njihove zlorabe.

Znanje tega sklopa je hkrati odskočna deska. Na strukturo, ki jo postavi HTML, se v praksi vežejo slogi za oblikovanje in programska logika, predvsem pa vsebine, ki jih je treba varovati. Prav zato se učbenik v naslednjem sklopu posveti kibernetski varnosti, s katero zgrajene rešitve zaščitimo pred grožnjami digitalnega okolja.

Univerzitetna založba
Univerze v Mariboru

Viri

Berners-Lee, T. in Connolly, D. W. (1995). Hypertext Markup Language – 2.0 (RFC 1866). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc1866

McCarron, S. in Ishikawa, M. (2010). XHTML 1.1 – Module-based XHTML (2. izd.) (W3C Recommendation). World Wide Web Consortium. https://www.w3.org/TR/xhtml11/

NSA. (2025). Različice jezika HTML. https://nsa-splet.si/html/uvod/html-uvod-04-razlicice.php

Pemberton, S., Austin, D., Axelsson, J., Çelik, T., Dominiak, D., Elenbaas, H., Epperson, B., Ishikawa, M., Matsui, S., Navarro, S., Relyea, D., Schnitzenbaumer, B., Smith, L., Spero, S., Stark, P., Stearns, M., Teague, J., Wugofski, T., Young, M. in Jacobs, I. (2002). XHTML 1.0: The Extensible HyperText Markup Language (2. izd.) (W3C Recommendation). World Wide Web Consortium. https://www.w3.org/TR/xhtml1/

Raggett, D. (1997). HTML 3.2 reference specification (W3C Recommendation). World Wide Web Consortium. https://www.w3.org/TR/2018/SPSD-html32-20180315/

Raggett, D., Le Hors, A. in Jacobs, I. (1999). HTML 4.01 specification (W3C Recommendation). World Wide Web Consortium. https://www.w3.org/TR/html401/

Web Hypertext Application Technology Working Group. (2025). HTML: Living standard – multipage version. https://html.spec.whatwg.org/multipage/

World Wide Web Consortium. (2025). W3C markup validation service. https://validator.w3.org/

3. SKLOP
KIBERNETSKA VARNOST

Zaščitimo informacije. Zavarujemo organizacije.

Kibernetska varnost je ključna za zaščito informacij, omrežij in sistemov pred grožnjami v digitalnem svetu. Razumemo grožnje, tveganja in ukrepe – na ravni organizacij, držav in mednarodnih povezav.



TIPIČNE INFORMACIJSKO-KIBERNETSKE GROŽNJE

PHISHING
Prevarantska sporočila, ki ciljajo na pridobitev občutljivih podatkov (gesla, bančni podatki ...).

MALWARE
Zlonamerna programska oprema, ki okuži ali poškoduje sisteme.

RANSOMWARE
Zlonamerna programska oprema, ki zaklene podatke in zahteva odkupnino.

APT (NAPREDNE TRAJNE GROŽNJE)
Ciljani napadi, ki so dolgotrajni, sofisticirani in običajno sponzorirani s strani držav.

DDoS NAPADI
Preobremenitev storitev z velikim številom zahtev in onemogočanje delovanja.

IZGUBA PODATKOV
Izguba, kraja ali nenamerna izbris podatkov zaradi napak, napadov ali nesreč.

POJMI V KIBERNETSKI VARNOSTI

ZAUPNOST (C)
Informacije so dostopne samo tistim, ki so pooblaščeni.

CELOVITOST (I)
Informacije so točne, nespremenjene in zanesljive.

RAZPOLOŽLJIVOST (A)
Informacije in sistemi so dostopni, ko jih potrebujemo.

TVEGANJE
Možnost, da grožnja izkoristi ranljivost in povzroči škodo.

UKREPI
Tehnični, organizacijski in kadrovski ukrepi za zmanjšanje tveganj.

ODZIV IN OBNOVA
Zaznava, odziv na incidente, obnova in učenje iz izkušenj.

UREDITEV KIBERNETSKE VARNOSTI

NATO
- Politike in strategije
- Skupni standardi
- Zavezniška sodelovanja

EVROPSKA UNIJA
- NIS2 direktiva
- DORA uredba
- ENISA smernice
- GDPR varstvo podatkov

REPUBLIKA SLOVENIJA
- Zakon o informacijski varnosti (ZInfV)
- SI-CERT
- NKS organizacija
- Varovanje kritične infrastrukture

KIBERNETSKA VARNOST = EKIPNO DELO

LJUDJE | PROCESI | TEHNOLOGIJA | ZAVEDANJE

NAČELA VARNEGA RAVNANJA

- Uporabljaj močna gesla in MFA
- Bodi previden pri povezavah in priponkah
- Posodabljaj sisteme in aplikacije
- Izobražuj se in poroča o incidentih
- Varuj osebne in občutljive podatke

ŽIVLJENJSKI CIKEL KIBERNETSKEGA INCIDENTA

ZAZNAJ – Odkrij grožnjo ali dogodek.
→ **ANALIZIRAJ** – Oceni vpliv in razlog dogodka.
→ **ODZOVI SE** – Ukrepi za omejitev škode.
→ **OBNOVI** – Povrni sisteme in podatke.

VARNOST NI IZDELEK, TEMVEČ PROCES.

ODGOVORNOST VSAKEGA IZMED NAS.

KLJUČNI UKREPI ZA ORGANIZACIJE

UPRAVLJANJE TVEGANJ
Redno ocenjuj in obvladuj tveganja.

KONTROLA DOSTOPA
Dostop omogočaj le pooblaščenim.

NADZOR IN ZAZNAVANJE
Spremljaj omrežje in sisteme ter zaznaj anomalije.

VARNOSTNO KOPIRANJE
Redno izdeluj varnostne kopije in jih testiraj.

ZAVEDANJE UPORABNIKOV
Usposabljaj zaposlene in krepi kulturo varnosti.

SKLADNOST
Upoštevaj zakone in standarde.

DOBRA KIBERNETSKA VARNOST = ZAVAROVANE INFORMACIJE + ZAŠČITENE ORGANIZACIJE + ZANESLJIVO DELOVANJE

Razumevanje groženj, pravilna uporaba tehnologije in odgovorno vedenje nas varujejo danes in v prihodnosti.

Univerzitetna založba
Univerze v Mariboru

1 Uvod

Digitalna preobrazba spreminja družbo na vseh ravneh, od posameznika prek skupin in organizacij do mest, regij in celo globalnih razmerij. Ne odpira le možnosti za nov tehnološki razvoj, temveč preoblikuje tudi tradicionalne družbene strukture, institucije in organizacije. Tehnologija in družba se vse bolj prepletata, zato postajajo problemi, s katerimi se srečujejo posamezniki, organizacije in družba kot celota, vse kompleksnejši, njihovo reševanje pa vse zahtevnejše. V poslovnem pogledu je digitalna preobrazba vrsta poslovne preobrazbe, ki jo poganjajo nastajajoče tehnologije. Tehnologija pri tem ni več zgolj podporna funkcija poslovnih procesov, saj omogoča nove in inovativne poslovne modele, spodbuja rast prodaje in lahko postane vir konkurenčne prednosti. Med trendi, ki digitalno preobrazbo spodbujajo, so družbena omrežja, mobilnost, internet stvari (angl. *Internet of Things, IoT*), kibernetska varnost, velike količine podatkov in analitika, računalništvo v oblaku, robotska avtomatizacija procesov, umetna inteligenca (predvsem strojno učenje) in veriženje blokov (angl. *Blockchain*). Prav te tehnologije so danes hrbtenica sodobne logistike, od pametnih skladišč in transportnih sistemov do sledenja pošiljkam. Medtem ko državam in organizacijam omogočajo večjo učinkovitost in inovacije, hkrati povečujejo površino napadov ter jih izpostavljajo novim varnostnim grožnjam (povzeto po Plevnik in Ščavničar, 2026).

Digitalno preobrazbo spremljata nenehen razvoj in uvajanje nove programske opreme, zato mora biti varnost vgrajena v celoten razvojni proces. Le tako se tveganje varnostnih pomanjkljivosti zmanjša že ob nastanku rešitve. Država in njena kritična infrastruktura sta že dlje časa tarča državnih in nedržavnih akterjev. Zaščita kritične infrastrukture predstavlja celovit konceptualni okvir za obvladovanje tveganj, ranljivosti in groženj, ki izhajajo iz medsebojno povezanih družbenih in tehničnih sistemov. Kritičnost teh sistemov izhaja iz posledic, ki bi jih njihove motnje ali uničenje imele za državo, naj gre za človeške in materialne izgube ali za izgubo ugleda in zaupanja. V kritično infrastrukturo sodi tudi velik del logistične infrastrukture, denimo pristanišča, železniška vozlišča in

distribucijski centri, zato izpad informacijskih sistemov na tem področju neposredno ogrozi oskrbo gospodarstva in prebivalstva.

Kibernetski sektor je postal pomemben dejavnik varovanja kritične infrastrukture in hkrati vprašanje, ki presega meje posameznih sektorjev. Njegov vzpon je prinesel pomembne spremembe. Uspešna izvedba digitalne preobrazbe zahteva celovit pristop k varnosti, ki poleg tehnologije vključuje tudi ljudi in postopke. Zagotavljanje kibernetske varnosti v spreminjajočem se digitalnem okolju temelji na rednem ocenjevanju tveganj, izvajanju varnostnih preizkusov in stalnem izobraževanju. Kibernetske grožnje so vse kompleksnejše, uničevalnejše, agresivnejše in pogostejše. Kibernetski prostor je ogrožen ves čas, zlonamerni dogodki pa se v njem dogajajo vsak dan, od napadov na nizki ravni do tehnološko izpopolnjenih operacij. To še posebej velja za oskrbovalne verige, ki so privlačna tarča, ker povezujejo veliko število partnerjev z zelo različnimi ravnmi zaščite. Odzivanje zato sloni na krepitvi odkrivanja, preprečevanja in odzivanja na zlonamerne kibernetske dejavnosti na nacionalni in nadnacionalni ravni.

Razumevanje sodobne odvisnosti od kibernetskega prostora postaja vse pomembnejši del našega vsakdana. Tehnološki napredek in povezanost z digitalnim svetom sta v veliki meri preoblikovala način življenja in dela ter medsebojno komunikacijo. Z izjemno rastjo interneta, pametnih naprav in oblačnih storitev je svet globoko vpet v mrežo virtualnih interakcij, ki oblikujejo naše vsakodnevne izkušnje. Enako velja za tok blaga, ki ga brez digitalnega toka informacij praktično ni več mogoče upravljati. V ospredje teh tehnoloških prelomnic stopajo raziskave, ki skušajo po eni strani razložiti vpliv nove realnosti na človekovo zasebnost in varnost, po drugi strani pa odgovoriti na vprašanje, ali tehnologija krepi ali omejuje našo sposobnost za inovacije in ustvarjalnost v delovnem in osebnem življenju. Tehnološki napredek namreč ponuja tako izhodišča za številne priložnosti kot tudi razmislek o ravnotežju trajnostnega razvoja vse bolj digitalizirane družbe.

Univerzitetna založba
Univerze v Mariboru

2 Teoretično razumevanje kibernetskega področja

Teoretično razumevanje kibernetskega področja kot ene izmed domen družbenega okolja je temelj za zaščito informacijskih sistemov in kritične infrastrukture pred naraščajočimi kibernetskimi grožnjami. Hkrati omogoča razvoj učinkovitih strategij in politik za zagotavljanje nacionalne varnosti in obrambe v digitalno povezanem svetu. Kibernetski prostor je kompleksen in se nenehno spreminja, zato brez teoretične podlage ni mogoče dosledno upravljati in varovati informacijskih sistemov, na katerih temeljijo tudi logistični procesi, od naročanja in skladiščenja do dostave. Kdor razume povezave med informacijsko zagotovitvijo, informacijsko varnostjo, kibernetsko varnostjo in kibernetsko obrambo, lažje dojame, kako se ta področja prepletajo in medsebojno podpirajo. Teoretično znanje omogoča prepoznavanje in razumevanje različnih vrst kibernetskih groženj, ki se hitro razvijajo, so tehnično napredne, pogosto čezmejne in lahko povzročijo obsežno škodo na informacijskih sistemih in infrastrukturi. Na tem znanju gradimo učinkovite strategije za preprečevanje groženj in odzivanje nanje. Teorija prav tako omogoča celosten in sistematičen pristop k zagotavljanju kibernetske varnosti, ki je bistven za zaščito kritične infrastrukture in občutljivih informacij. Za nacionalno varnost in obrambno načrtovanje je pomembno tudi razumevanje vloge in odgovornosti oboroženih sil na tem področju, za gospodarstvo pa zavedanje, da so v isti sistem varovanja vpete tudi organizacije, ki upravljajo oskrbovalne verige. Vse to kaže, kako pomembno je teoretično znanje za oblikovanje učinkovitih politik, strategij in ukrepov na področju kibernetske varnosti in obrambe (povzeto po Plevnik in Ščavničar, 2026).

V tem poglavju bomo najprej analizirali pomen kibernetskega prostora, nato opredelili osnovne pojme njegovega varovanja in na koncu predstavili kibernetske grožnje s poudarkom na tistih, ki ogrožajo organizacije in oskrbovalne verige.

2.1 Kibernetski prostor

Kibernetski prostor je v času digitalne preobrazbe postal osrednji element medsebojnega povezovanja, komunikacije in izmenjave informacij, tudi v oskrbovalnih verigah, kjer se prek njega usklajujejo naročila, zaloge in prevozi. Enotne opredelitve ni. Različni viri in standardi ponujajo svoje definicije ter pri tem poudarjajo njegovo kompleksnost in globalno naravo. Zaradi pomena za sodobne družbe ga zakonodaja, mednarodne organizacije in obrambni viri obravnavajo kot eno od osrednjih področij delovanja. Nato (2016a) ga priznava kot samostojno domeno operativnega delovanja in ga vključuje v koncept kolektivne obrambe. Temeljito razumevanje njegovih plasti in dimenzij oblikovalcem politik ter strokovnjakom za varnostna in obrambna vprašanja omogoča, da razvijajo strategije, ki se učinkovito odzivajo na izzive tega kompleksnega in dinamičnega digitalnega okolja (povzeto po Plevnik in Ščavničar, 2026).

Mednarodna organizacija za standardizacijo (angl. *International Organization for Standardization*, v nadaljevanju ISO) v standardu ISO/IEC TS 27100:2020 kibernetski prostor opredeli kot medsebojno povezano digitalno okolje omrežij, storitev, sistemov, ljudi, procesov in organizacij ter vsega, kar se v tem okolju nahaja ali skozenj prehaja (ISO/IEC, 2020). Ameriški National Institute of Standards and Technology (v nadaljevanju NIST) ponudi tehnično celovito opredelitev, po kateri je kibernetski prostor globalna domena v informacijskem okolju, ki jo sestavlja soodvisno omrežje infrastruktur informacijskih sistemov, vključno z internetom, telekomunikacijskimi omrežji, računalniškimi sistemi ter vgrajenimi procesorji in krmilniki (NIST, 2012). Preprostejša je opredelitev Oxfordskega slovarja, po kateri je kibernetski prostor namišljen prostor brez fizične lokacije, v katerem poteka komunikacija prek računalniških omrežij (Oxford University Press, 2023). Za potrebe tega učbenika velja izpostaviti še dve opredelitvi. Nato je v sporočilu z vrha v Varšavi zapisal, da kibernetski prostor postaja področje operativnega delovanja, v katerem se mora zavezništvo braniti enako učinkovito kot v zraku, na kopnem in na morju, s čimer ohranja svobodo delovanja in odločanja v vseh okoliščinah (NATO, 2016a). V slovenski zakonodaji pa je Zakon o informacijski varnosti (v nadaljevanju ZInfV, 2018) kibernetski prostor opredelil kot globalno informacijsko okolje, ustvarjeno s pomočjo elektronskih komunikacijskih omrežij in informacijskih sistemov, ki omogoča nastanek, obdelavo in izmenjavo informacij. Novi Zakon o informacijski varnosti opredelitev posodablja in kibernetski prostor določa kot globalno informacijsko okolje, ki ga tvorijo informacijski sistemi in omrežja, podatki, digitalne naprave in njihovi uporabniki (ZInfV-1, 2025).

Predstavljene opredelitve kažejo, da je kibernetski prostor postal osrednji element povezovanja, komunikacije in izmenjave informacij. Institucije in dokumenti ga opredeljujejo na več načinov, ki odražajo njegovo kompleksnost in globalni pomen. V splošnem ga razumemo kot obsežno, medsebojno povezano digitalno okolje, v katerem se prepletajo tehnološke, organizacijske in človeške sestavine. Vse več poudarka je na njegovem operativnem vidiku, saj ga varnostne in obrambne institucije obravnavajo kot eno od osrednjih področij delovanja, kar je pomembno za nacionalno in mednarodno politiko. Raznolikost opredelitev ni pomanjkljivost. Vsaka osvetli svoj vidik, zgradbo, delovanje ali pomen za kibernetsko varnost, skupaj pa omogočajo celostno razumevanje tega dinamičnega in vseprisotnega okolja, v katerem danes poteka tudi pretežni del logističnega poslovanja.

K opredelitvi kibernetskega prostora sodijo tudi njegove značilnosti, ki jih izpostavlja Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-2, 2019). To so globalnost, asimetričnost in horizontalnost. V praksi to pomeni, da kibernetski prostor ne pozna geografskih in časovnih omejitev, da je dejanski vir in akterja ogrožanja težko določiti ter da v njem delujejo tako državni kot nedržavni akterji. Prav zaradi teh značilnosti se lahko napad na oskrbovalno verigo začne kjerkoli na svetu in kadarkoli. Zgradbo kibernetskega prostora najpogosteje opišemo s tremi plastmi, fizično (angl. *Physical Layer*), logično (angl. logical layer) in plastjo kibernetske osebnosti (angl. *Cyber Persona Layer*) (NATO, 2020) (glej Sliko 1).



Slika 2: Tri plasti kibernetskega prostora.
Vir: NATO, 2020.

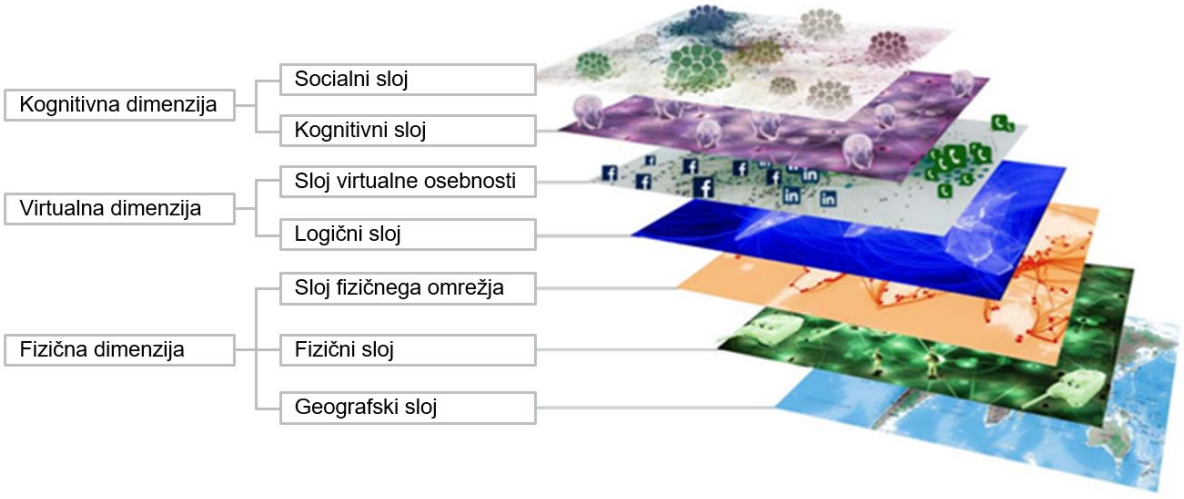
Fizično plast sestavljajo naprave informacijske tehnologije in infrastruktura v fizičnem okolju, ki omogoča shranjevanje, prenos in obdelavo informacij v kibernetskem prostoru, vključno s podatkovnimi skladišči in povezavami, po katerih podatki potujejo med omrežnimi komponentami (U.S. Department of Defense [DoD], 2018). Mednje sodijo

strojna oprema in infrastruktura, na primer računalniške naprave, naprave za shranjevanje podatkov, omrežne naprave ter žične in brezžične povezave. V logističnem okolju so del te plasti tudi skladiščni terminali, čitalniki črtnih kod in strežniki, na katerih tečejo sistemi za vodenje skladišč in prevozov. Fizična raven omrežja je prva referenčna točka za določitev geografske lokacije in s tem ustreznega pravnega okvira. Čeprav je v kibernetskem prostoru geopolitične meje mogoče prestopiti zlahka in hitro, ostajajo vprašanja suverenosti vezana na fizične domene. Vsaka fizična komponenta kibernetskega prostora je poleg tega v lasti javnega ali zasebnega subjekta, ki lahko dostop do nje nadzoruje ali omejuje.

Logično plast tvorijo elementi omrežja, ki so med seboj povezani neodvisno od fizičnega omrežja, saj njihova povezanost temelji na logičnem programiranju, ki poganja omrežne komponente (DoD, 2018). Odnosi med elementi niso nujno vezani na določeno fizično povezavo ali vozlišče, temveč na njihovo zmožnost logičnega naslavljanja ter izmenjave in obdelave podatkov. V logični plasti so predstavljene posamezne povezave in vozlišča, pa tudi porazdeljeni elementi kibernetskega prostora, kot so podatki, aplikacije in omrežni procesi, ki niso vezani na eno samo vozlišče. Tak porazdeljen element je na primer sistem za sledenje pošiljkam, ki podatke zbira iz več virov in jih uporabnikom prikazuje ne glede na to, kje se ti fizično nahajajo.

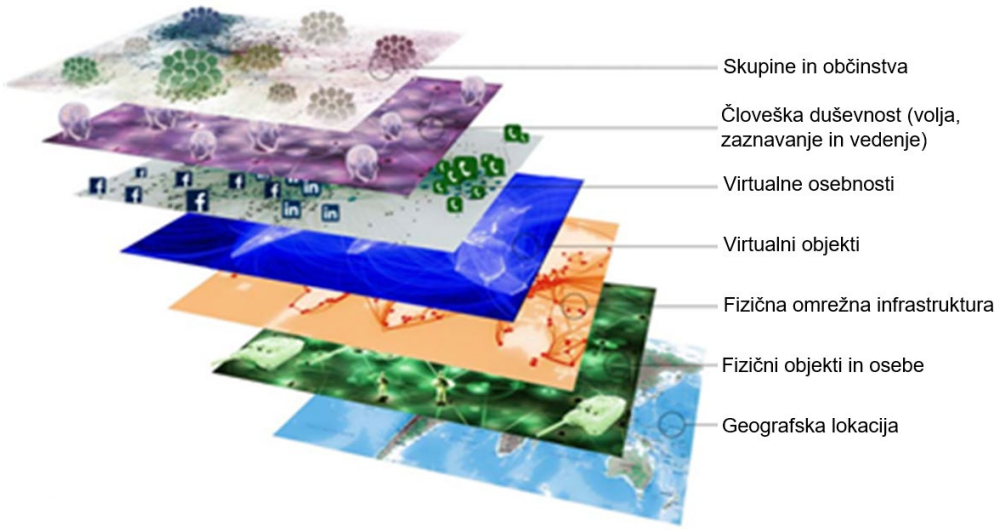
Plast kibernetske osebnosti je pogled na kibernetski prostor, ki nastane z izločanjem podatkov iz logične plasti (DoD, 2018). S pravili logične plasti se oblikujejo opisi digitalnih predstavitev identitete akterja ali entitete v kibernetskem prostoru, torej kibernetske osebnosti. To plast sestavljajo uporabniški računi v omrežju ali informacijski tehnologiji, človeški ali avtomatizirani, in njihova medsebojna razmerja. Kibernetske osebnosti se lahko neposredno nanašajo na dejansko osebo ali subjekt ter vključujejo nekatere osebne ali organizacijske podatke, kot so naslovi elektronske pošte, naslovi IP, spletne strani, telefonske številke, prijave na spletne forume ali gesla za finančne račune. Posameznik lahko ustvari in vzdržuje več kibernetskih osebnosti z različnimi identifikatorji, na primer ločena službeni in osebni naslov elektronske pošte ali različne identitete v spletnih forumih, klepetalnicah in družabnih omrežjih, ki se lahko razlikujejo po stopnji dejanske točnosti. Zato uporaba kibernetskih osebnosti otežuje ugotavljanje odgovornosti za dejanja v kibernetskem prostoru. V poslovnem in logističnem okolju so del te plasti tudi računi zaposlenih v portalih za naročanje in izmenjavo dokumentov, zato je njihova zloraba ena najpogostejših vstopnih točk napadalcev.

Podrobnejšo razdelitev kibernetskega prostora zagovarjajo Ducheine idr. (2017), ki ga razčlenijo na fizično dimenzijo (angl. *Physical Dimension*), virtualno dimenzijo (angl. *Virtual Dimension*) in kognitivno dimenzijo (angl. *Cognitive Dimension*) (glej Sliko 2). Fizična dimenzija vključuje geografski sloj (angl. *Geographical Layer*), fizični sloj (angl. *Physical Layer*) in sloj fizičnega omrežja (angl. *Physical Network Layer*). Virtualna dimenzija zajema logični sloj (angl. *Logical Layer*) in sloj virtualne osebnosti (angl. *Virtual Persona Layer*). Kognitivna dimenzija pa združuje kognitivni sloj (angl. *Cognitive Layer*) in socialni sloj (angl. *Social Layer*).



Slika 3: Dimenzije in sloji.
Vir: Ducheine idr., 2017.

Vsak sloj vsebuje entitete, ki so potrebne za operacionalizacijo koncepta plasti in na katere je mogoče vplivati z dejavnostmi ali operacijami (glej Sliko 3) (Ducheine idr., 2017). Geografski sloj vključuje geografske lokacije. Fizični sloj zajema fizične predmete in osebe, sloj fizičnega omrežja pa fizično omrežno infrastrukturo, kot so usmerjevalniki, kabli in računalniki. Logični sloj vključuje virtualne predmete, na primer programsko opremo, sloj virtualnih osebnosti pa virtualne osebe, kot so profili na družbenih medijih in poštni računi. Kognitivni sloj zajema človeško duševnost, torej voljo, zaznavanje in vedenje, socialni sloj pa skupine in občinstva, ki se v omrežjih povezujejo in sodelujejo. Entitete so medsebojno povezane in soodvisne, saj sprememba ene vpliva tudi na druge. To soodvisnost dobro ponazarja logistični primer. Izpad usmerjevalnika v skladišču kot entitete fizičnega omrežja ustavi programsko opremo za vodenje zalog v logičnem sloju, s tem onemogoči delo skladiščnikov v kognitivnem sloju in poruši usklajenost celotne verige partnerjev v socialnem sloju.



Slika 4: Entitete.
Vir: Ducheine idr., 2017.

Kibernetski prostor je v digitalni preobrazbi postal osrednji element medsebojnega povezovanja, komunikacije in izmenjave informacij, njegov vpliv pa presega tradicionalne fizične meje. Prav zato mu zakonodaja, mednarodne organizacije in obrambni viri pripisujejo velik pomen in nujnost za delovanje sodobne družbe. V njem se prepletajo fizična plast, logična plast in plast kibernetske osebnosti, ki skupaj tvorijo dinamično digitalno okolje. Kibernetski prostor torej ni zgolj tehnična domena, ampak prostor, v katerem človeška interakcija in politične strategije oblikujejo digitalno prihodnost. Za logistiko to pomeni, da zanesljivost oskrbovalnih verig ni odvisna samo od opreme in programov, temveč tudi od ljudi, ki sisteme uporabljajo, in od pravil, ki urejajo njihovo delovanje.

2.2 Razmerja med pojmi varovanja kibernetskega prostora

Opredelitev razmerij med pojmi, povezanimi z varovanjem kibernetskega prostora, je izjemno pomembna, saj jasne definicije strokovnjakom, politikom in uporabnikom omogočajo učinkovito komunikacijo o kompleksnih in pogosto prekrivajočih se vprašanjih. Poenoteni pomeni izrazov zmanjšujejo zmedo in izboljšujejo sodelovanje. Organizacija, ki pomensko raznolikost izrazov jasno opredeli, lažje uskladi svoje politike in postopke ter zagotovi, da zaposleni razumejo, kaj se od njih pričakuje v okviru njihovih vlog. To velja tudi za logistična podjetja, v katerih se varnostne naloge delijo med informatike, skladiščno in transportno osebje ter vodstvo. Razumevanje razlik med izrazi je tudi podlaga za razvoj učinkovitih izobraževalnih programov, s katerimi osebje pridobi potrebna znanja in veščine za zaščito kibernetskega prostora. Usklajene opredelitve industriji omogočajo razvoj standardov in najboljših praks, ki so jasni, dosledni in široko

sprejeti, organizacijam pa boljše obvladovanje tveganj in učinkovitejše odzivanje na varnostne incidente. Jasne definicije so potrebne tudi za oblikovanje učinkovite zakonodaje in pravnih okvirov, ki ustrezno naslavljajo različne vidike kibernetske varnosti in obrambe. Ker kibernetski prostor ne pozna meja, je na globalni ravni pomembno, da države in mednarodne institucije težijo k enotnemu razumevanju pojmov ter tako lažje sodelujejo v mednarodnih prizadevanjih za krepitev kibernetske varnosti. Jasno razlikovanje med pojmi je zato temelj uspešnega oblikovanja in izvajanja strategij za varovanje kibernetskega prostora (povzeto po Plevnik in Ščavničar, 2026).

Pri varovanju kibernetskega prostora je bistveno razumeti razmerja med pojmi, kot so informacijska zagotovitev, informacijska varnost, kibernetska varnost in kibernetska obramba. Celosten pogled na obravnavo kibernetskih tveganj in potreb ponuja tudi hierarhična razvrstitev potreb v kibernetskem prostoru, ki jo je po zgledu Maslowove piramide potreb razvila ENISA (2017) (glej Sliko 4). Hierarhična razvrstitev potreb v kibernetskem prostoru je pomembna zaradi:

- prioritizacije varnostnih ukrepov,
- razumevanja vpliva na posameznike in družbo,
- celostnega pristopa k obravnavi tveganj,
- podlage za oblikovanje politik,
- razvoja in vzdrževanja zaupanja v digitalno okolje ter
- strateškega načrtovanja in dodeljevanja virov.

Takšen hierarhičen prikaz organizacijam in državam omogoča, da razvijajo in vzdržujejo zaupanje v digitalno okolje ter učinkovito načrtujejo in dodeljujejo vire za zaščito kibernetskega prostora. Temeljne potrebe, kot je osnovna varnost kibernetskega prostora, morajo biti izpolnjene, preden se lahko naslovijo višje ravni, na primer zaščita enotnega digitalnega trga. Hierarhija hkrati poudarja, da kibernetska varnost ne vpliva le na posamezne uporabnike interneta, ampak na širšo družbo, vključno z vprašanji demokracije in človekovih pravic. Podobno kot Maslowova piramida ponuja celosten pogled na človeške potrebe, hierarhična razvrstitev v kibernetskem prostoru zagotavlja strukturiran pristop k obravnavi različnih ravni kibernetskih tveganj in potreb ter služi kot okvir za oblikovanje nacionalnih in mednarodnih politik kibernetske varnosti. S tem se zagotovi, da so ukrepi usmerjeni najprej v zaščito temeljnih potreb in šele nato v spodbujanje višjih ciljev, kot sta demokracija in človekove pravice. Enaka logika velja v praksi posamezne organizacije. Logistično podjetje mora najprej zavarovati osnovno delovanje svojih sistemov za skladiščenje in prevoz ter šele nato vlagati v naprednejše cilje, na primer v

digitalne inovacije in nove storitve. Hierarhična struktura torej ni samo teoretični model, ampak praktično orodje za izboljšanje kibernetske varnosti na vseh ravneh družbe ter za strateško načrtovanje in učinkovito dodeljevanje virov.



Slika 5: Hierarhična razvrstitev potreb v kibernetskem prostoru po Maslowu.
Vir: ENISA, 2017.

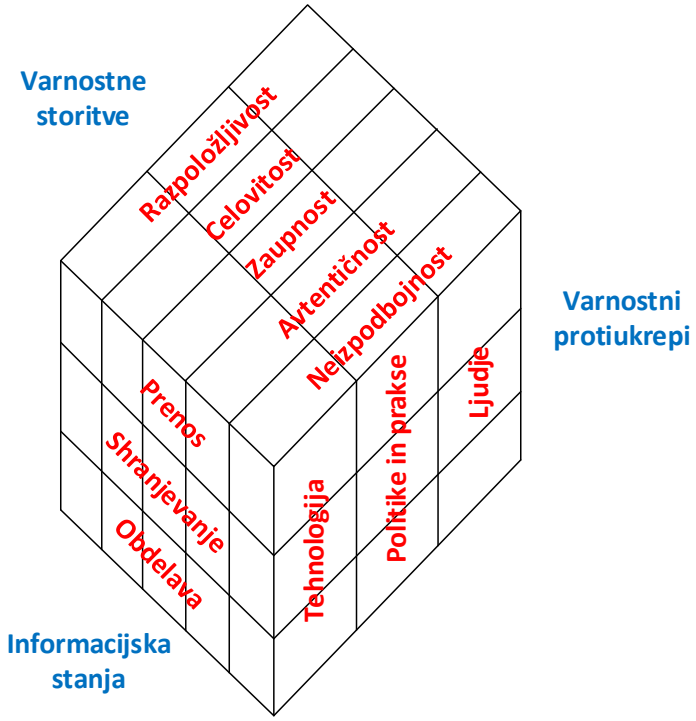
Slika 4 prikazuje pogled ENISE (2017) na potrebe v kibernetskem prostoru. Hierarhija se na vrhu začne s temeljnimi vrednotami EU, kot so demokracija in človekove pravice, ter se nadaljuje navzdol do osnovnih potreb državljanov. Med ravnmi obstajajo soodvisnosti. Zaščita kritične informacijske infrastrukture je temeljna podlaga za uspeh enotnega digitalnega trga, ki povezuje podjetja in državljane, med njimi tudi ponudnike in uporabnike logističnih storitev, ki poslujejo čezmejno. Kibernetske varnosti državljanov, infrastrukture in podjetij v sedanjih razmerah ni mogoče doseči zunaj globaliziranega okvira. Zato je treba vzpostaviti kibernetsko diplomacijo kot sredstvo za preprečevanje groženj ter za obrambo in zaščito EU, njenih državljanov, infrastruktur in podjetij. Ob tem velja opozoriti, da je treba temeljne vrednote in norme EU, vključno z etiko, upoštevati na vseh ravneh kibernetskega prostora oziroma pri vseh izdelkih in storitvah, ki so na voljo strankam v EU, ne glede na to, kje na svetu so bili proizvedeni ali razviti.

V tem podpoglavju bodo opredeljena razmerja med pojmi varovanja kibernetskega prostora, kot so informacijska zagotovitev, informacijska varnost, kibernetska varnost in kibernetska obramba. Na podlagi teoretičnih opredelitev bomo oblikovali delovne opredelitve posameznih pojmov, kot jih bomo uporabljali v tem učbeniku.

2.2.1 Zagotavljanje informacijske varnosti

Opredelitev informacijske zagotovitve je za organizacije osrednjega pomena, saj ponuja celovit okvir za zaščito informacij v vseh oblikah in s tem podpira zaupanje ter zanesljivost v digitalnem okolju. Organizacijam omogoča, da učinkovito upravljajo tveganja, poslujejo skladno z zakonodajo, se zanesljivo odzivajo na incidente in ohranjajo neprekinjeno poslovanje, kar je v hitro spreminjajočem se tehnološkem svetu pogoj za vzpostavitev in ohranjanje konkurenčne prednosti. V logistiki, kjer zamuda informacije pomeni zamudo blaga, je neprekinjeno poslovanje še posebej občutljivo. Informacijska zagotovitev je zato temeljna sestavina strateškega upravljanja in načrtovanja, ki organizacijam omogoča, da se prilagajajo in inovirajo ter hkrati zaščitijo svoje najpomembnejše informacijske vire (povzeto po Plevnik in Ščavničar, 2026).

Za boljše razumevanje kompleksnosti informacijske zagotovitve v nadaljevanju predstavljamo model, ki ponuja celovit okvir za razumevanje in izvajanje varnostnih strategij v informacijskih sistemih. Tridimenzionalni model informacijske zagotovitve (Maconachy idr., 2021) (glej Sliko 5) na prvi dimenziji prikazuje varnostne storitve (angl. *Security Services*), med katere sodijo razpoložljivost (angl. *Availability*), celovitost (angl. *Integrity*), overitev (angl. *Authentication*), zaupnost (angl. *Confidentiality*) in neprikrivanje (angl. *Non Repudiation*). Druga dimenzija zajema varnostne protiukrepe (angl. *Security Countermeasures*), razdeljene na tehnologijo (angl. *Technology*), politike in prakse (angl. *Policy and Practice*) ter ljudi (angl. *People*). Tretja dimenzija prikazuje informacijska stanja (angl. *Information States*), torej prenos (angl. *Transmission*), shranjevanje (angl. *Storage*) in obdelavo (angl. *Processing*). Model ponuja celosten pogled na informacijsko varnost, saj združuje varnostne storitve, ki jih je treba zagotavljati z varnostnimi protiukrepi, in različna stanja, v katerih se informacije lahko nahajajo. S tem pomaga pri načrtovanju in uvajanju varnostnih strategij, ki upoštevajo tehnološke rešitve, politike in postopke ter vlogo ljudi. Uporabo modela si v logistiki zlahka predstavljamo. Podatek o pošiljki je treba zavarovati, ko potuje med partnerji, ko je shranjen v skladiščnem sistemu in ko se obdeluje ob pripravi naročila, pri čemer tehnologija, pravila in usposobljeni ljudje skupaj skrbijo za njegovo zaupnost, celovitost in razpoložljivost.



Slika 6: Model informacijske zagotovitve.
Vir: Maconachy idr., 2021.

V literaturi najdemo vrsto opredelitev informacijske zagotovitve, ki se bolj ali manj osredotočajo na razpoložljivost, celovitost in zaupnost informacij v informacijskih sistemih. Izpostavljamo dve opredelitvi, ki sta pomembni za razumevanje področja. Oba vira veljata za avtoritativna, saj se njuni opredelitvi v literaturi pogosto uporabljata kot standard ali referenca in zajemata bistvene vidike informacijske zagotovitve, pomembne za večino scenarijev in aplikacij. Odbor za varnost informacijskih sistemov informacijsko zagotovitev v širšem smislu opredeli kot informacijske operacije, ki varujejo in branijo informacije ter informacijske sisteme in s tem zagotavljajo njihovo razpoložljivost, celovitost, zaupnost, verodostojnost in nepreklicnost, vključno z obnovo informacijskih sistemov prek zmogljivosti za zaščito, odkrivanje in odzivanje (Maconachy idr., 2021). NIST (2003) informacijsko zagotovitev v ožjem smislu opredeli kot ukrepe za zaščito in obrambo informacij in informacijskih sistemov, ki zagotavljajo njihovo razpoložljivost, celovitost, verodostojnost, zaupnost in nepreklicnost. Tudi ti ukrepi vključujejo ponovno vzpostavitev informacijskih sistemov z zmogljivostmi za zaščito, odkrivanje in odzivanje.

Iz navedenih opredelitev izpeljemo delovno opredelitev, ki jo bomo uporabljali v nadaljevanju za razumevanje področja. Informacijska zagotovitev je širok pojem, ki zajema ukrepe za zaščito in zanesljivost informacij. Ne omejuje se na preprečevanje napadov ali nepooblaščenih dostopov, temveč vključuje tudi zagotavljanje celovitosti, razpoložljivosti, verodostojnosti in zaupnosti informacij. Tak pristop obsega fizično, tehnično in

administrativno varnost, upravljanje tveganj, skladnost s predpisi in tudi obnovo po incidentih. Za ta učbenik je delovna opredelitev bistvena, ker vzpostavlja jasnost osnovnih pojmov, na katerih gradijo nadaljnja poglavja. Za logistične organizacije pa je pomembna tudi praktično, saj pokriva celoten krog varovanja informacij o blagu in partnerjih, od preprečevanja vdorov do obnove sistemov po incidentu, ko mora oskrbovalna veriga čim prej spet steči.

2.2.2 Informacijska varnost

Opredelitev informacijske varnosti je temelj zaščite podatkov, saj zagotavlja zaupnost, celovitost in razpoložljivost informacij. Brez jasno določenih politik in postopkov so informacijski sistemi izpostavljeni grožnjam, kot so vdori, zlorabe podatkov ter izguba ali kraja informacij, kar lahko vodi do finančnih izgub, izgube zaupanja strank in škode za ugled organizacije. V logistiki, kjer si partnerji med seboj zaupajo podatke o naročilih, zalogah in pošiljkah, je tako zaupanje tudi pogoj za sodelovanje v oskrbovalni verigi. Informacijska varnost je poleg tega nujna za skladnost z zakonodajo in regulativnimi zahtevami, ki urejajo zaščito osebnih podatkov, ter z industrijskimi standardi. Vsi deležniki v organizaciji, od vodstva do zaposlenih, morajo jasno razumeti varnostna načela in svoje obveznosti, da lahko dejavno prispevajo k varovanju informacijskih sredstev. V dobi digitalizacije in nenehno razvijajočih se kibernetskih groženj je trdna informacijska varnost bistvena za neprekinjeno in varno poslovanje ter delovanje organizacije (povzeto po Plevnik in Ščavničar, 2026).

V literaturi najdemo vrsto opredelitev informacijske varnosti, ki se večinoma osredotočajo na varovanje informacij v različnih oblikah pred nepooblaščenim dostopom. Oxfordski slovar jo opredeli kot zaščito elektronskih informacij pred nepooblaščenim dostopom ali uporabo (OED, 2024). Wang in Wendy (2019) opredelitev razširita na varnost računalniških sistemov, pri čemer gre za zaščito pred razkritjem, samovoljnim spreminjanjem, nepooblaščenim dostopom, motenjem ali uničenjem, namen pa je zagotoviti celovitost, zaupnost in razpoložljivost informacij. Drugačen, ekonomski pristop ubereta Reid in van Niekerk (2014), ki v opredelitev vključita zaščito pred grožnjami s ciljem čim bolj zmanjšati tveganja poslovnih dejavnosti ter čim bolj povečati donosnost naložb, izkoriščanje poslovnih priložnosti in neprekinjenost poslovanja. Splošna opredelitev se nanaša na razpoložljivost, celovitost in zaupnost informacij (Solms in Solms, 2018), nekoliko razširjena pa te lastnosti upošteva ne glede na vrsto podatkov in ne glede na njihov vir, elektronski ali fizični (Andronache in Althonayan, 2018). Podoben pogled zagovarjata Maurer in Morgus (2014), ki informacijsko varnost povežeta s tehničnimi in upravnimi ukrepi. Reid in van Niekerk (2014) jo opredelita tudi prek

sistemov in strojne opreme, ki informacije uporabljajo, shranjujejo in prenašajo, z namenom zaščite informacij in njihovih najpomembnejših elementov. NIST informacijsko varnost opredeli kot zaščito informacij in informacijskih sistemov pred nepooblaščenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem zaradi zagotavljanja zaupnosti, celovitosti in razpoložljivosti (Paulsen in Byers, 2019). ENISA (2017) opredelitev nadgradi z zahtevo, da omrežja in sistemi na določeni ravni zaupanja kljubujejo naključnim dogodkom ter nezakonitim ali zlonamernim dejanjem, ki ogrožajo razpoložljivost, pristnost, celovitost in zaupnost shranjenih ali prenesenih podatkov in z njimi povezanih storitev. V slovenskem pravnem redu Zakon o informacijski varnosti (ZInfV, 2018) informacijsko varnost opredeljuje kot zaščito, varovanje in obrambo informacijskega okolja pred nedovoljenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem z namenom zagotavljanja zaupnosti, verodostojnosti, celovitosti in razpoložljivosti. Novi Zakon o informacijski varnosti opredelitev posodablja in jo veže na omrežne in informacijske sisteme ter pripadajoče podatke, ki jih je treba zaščititi pred nedovoljenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem, in sicer za zagotavljanje zaupnosti, avtentičnosti, celovitosti in razpoložljivosti teh sistemov in podatkov (ZInfV-1, 2025). Nato zagotavljanje informacijske varnosti opredeli kot zaščito in varovanje informacij ter informacijskih sistemov z zagotavljanjem njihove razpoložljivosti, celovitosti in zaupnosti (NATO, 2018a). Zanimivo je, da je Ministrstvo za obrambo Republike Slovenije (v nadaljevanju MORS) termin informacijske varnosti opredelilo zgodaj, ko se v Sloveniji še ni uveljavil, in sicer v pravilniku o delovanju komunikacijskega in informacijskega sistema (v nadaljevanju KIS) ministrstva (MORS, 2008). Ta opredelitev zajema določanje in uporabo ukrepov za varovanje tajnih podatkov, ki se obravnavajo v komunikacijskih, informacijskih in drugih elektronskih sistemih, pred naključno ali namerno izgubo tajnosti, celovitosti ali razpoložljivosti ter ukrepe za preprečevanje izgube celovitosti in razpoložljivosti samih sistemov.

Iz navedenih opredelitev smo izpeljali delovno opredelitev. Informacijska varnost zajema aktivnosti za zaščito podatkov in informacij pred nepooblaščenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem, pregledovanjem, snemanjem ali uničenjem, vključuje pa tudi fizično in kadrovsko varnost. Ta delovna opredelitev nam bo v nadaljevanju učbenika pomagala, da se osredotočimo na vidike, ki so pomembni za organizacije in njihove informacijske tokove. Za bralca s področja logistike je pri tem bistveno spoznanje, da informacijska varnost ne pokriva le računalnikov, ampak tudi dokumente v papirni obliki, ljudi in prostore, od prevoznih listin do dostopa v skladišče.

2.2.3 Kibernetska varnost

Opredelitev kibernetske varnosti zajema specifične strategije in ukrepe za zaščito računalniških sistemov, omrežij in podatkov pred kibernetskimi napadi in grožnjami, ki so vse pogostejše in naprednejše. V svetu, ki je vedno bolj povezan in odvisen od tehnologije, kibernetska varnost neposredno vpliva na ekonomsko stabilnost, nacionalno varnost in zaščito infrastrukture, vključno z logistično, ki poganja oskrbo gospodarstva. Bistvena je za vzpostavitev zaupanja v digitalne storitve, zagotavljanje skladnosti z zakonodajo ter zaščito intelektualne lastnine in zasebnosti posameznikov. Jasna opredelitev hkrati prispeva k razumljivi razdelitvi odgovornosti in pričakovanj med deležniki ter je podlaga za mednarodno sodelovanje pri obravnavi globalnih kibernetskih tveganj (povzeto po Plevnik in Ščavničar, 2026).

V literaturi najdemo vrsto opredelitev kibernetske varnosti, ki se bolj ali manj osredotočajo na varnost uporabnikov, strojne opreme, programske opreme, storitev in vseh informacij o njih v kibernetskem prostoru. Wang in Wendy (2019) kibernetsko varnost obravnavata kot varnost posameznikov in podjetij, ki jo dosegamo z zaščito pred varnostnimi kršitvami, incidenti in namernimi napadi na sisteme. Reid in van Niekerk (2014) opredelitev razširita na zaščito informacij in informacijskih sistemov, ki vključuje ohranjanje celovitosti, zaupnosti in razpoložljivosti informacijskih virov v kibernetskem prostoru. Natančnejša opredelitev zajema zaščito orodij, sistemov, procesov, konceptov, metod in strategij za varovanje lastnosti kibernetskega prostora pred nepooblaščenim dostopom in izgubo informacij, s čimer se ohranjajo celovitost, zaupnost in razpoložljivost virov (Andronache in Althonayan, 2018). Mednarodna telekomunikacijska zveza (angl. *International Telecommunication Union*, v nadaljevanju ITU) kibernetsko varnost opredeljuje kot zbirko orodij, politik, varnostnih konceptov, varnostnih varoval, smernic, pristopov k obvladovanju tveganja, ukrepov, usposabljanja, najboljših praks, zagotovil in tehnologij, ki se lahko uporabljajo za zaščito kibernetskega okolja ter sredstev organizacije in uporabnikov (Santos, 2020). Drugače jo opredelita Maurer in Morgus (2014), in sicer kot ukrepe za zagotavljanje prijazne uporabe računalniških sistemov in onemogočanje nepooblaščenega izkoriščanja informacij v njih. Celovita opredelitev pojma obsega zbirko politik, orodij, smernic, konceptov, pristopov, ukrepov, tehnologij, najboljših praks in usposabljanja, ki se uporabljajo za zaščito organizacijskih kibernetskih sredstev in uporabnikov (Reid in van Niekerk, 2014). NIST kibernetsko varnost opredeli kot sposobnost zaščite ali obrambe kibernetskega prostora pred kibernetskimi napadi (Paulsen in Byers, 2019). Celostna je opredelitev ENISE (2017), ki zajema vse vidike preprečevanja, napovedovanja, tolerance, odkrivanja, blaženja, odstranjevanja, analize in preiskovanja kibernetskih incidentov. Ob upoštevanju različnih komponent kibernetskega prostora

mora kibernetska varnost po tej opredelitvi zagotavljati razpoložljivost, zanesljivost, varnost, zaupnost, celovitost in vzdrževanje za materialne sisteme, informacije in omrežja, robustnost, preživetje in odpornost za podporo dinamičnosti kibernetskega prostora ter odgovornost, pristnost in nepreklicnost za podporo informacijski varnosti. V slovenski zakonodaji je kibernetska varnost opredeljena kot sposobnost zaščititi, varovati in braniti kibernetski prostor pred kibernetskimi grožnjami, incidenti in kibernetskimi napadi (ZInfV, 2018). Po novem zakonu so kibernetska varnost dejavnosti, ki so potrebne za zaščito omrežnih in informacijskih sistemov, uporabnikov takih sistemov in drugih oseb, na katere vplivajo kibernetske grožnje (ZInfV-1, 2025). Strategija kibernetske varnosti Republike Slovenije pa jo opredeli kot skupek aktivnosti in drugih tehničnih in netehničnih ukrepov, katerih namen je zaščititi računalnike, računalniška omrežja, strojno in programsko opremo ter informacije, ki jih ta vsebuje in obravnava, vključno s programsko opremo, podatki in drugimi elementi kibernetskega prostora, pred vsemi grožnjami, tudi grožnjami nacionalni varnosti (Vlada RS, 2016a).

Iz navedenih opredelitev izpeljemo delovno opredelitev. Kibernetska varnost zajema procese, aplikacije in storitve za zaščito uporabnikov, strojne opreme, programske opreme, storitev in vseh informacij o njih v kibernetskem prostoru. Ta opredelitev preprečuje morebitne nesporazume in napačne razlage. Za logistično organizacijo v praksi pomeni, da kibernetska varnost ne varuje samo računalnikov v pisarni, temveč tudi skladiščne terminale, sisteme za načrtovanje prevozov, portale za stranke in podatke, ki si jih podjetje izmenjuje s partnerji v oskrbovalni verigi.

2.2.4 Kibernetska obramba

Opredelitev kibernetske obrambe je pomembna za razumevanje kibernetskih groženj in učinkovito soočanje z njimi, saj določa obseg, metode in strategije za zaščito informacijskih sistemov. Jasna opredelitev organizacijam in vladam pomaga pri oblikovanju ustreznih politik, protokolov in varnostnih ukrepov za preprečevanje, odkrivanje in odzivanje na kibernetske napade. Različni avtorji kibernetsko obrambo uvrščajo bodisi v civilno bodisi v vojaško področje. V tem učbeniku jo bomo obravnavali predvsem znotraj vojaških struktur. V vojaškem kontekstu je kibernetska obramba pogosto povezana z visoko stopnjo tajnosti ter uporabo naprednih tehnologij in taktik. Zaradi mogočih posledic kibernetskih napadov na vojaške in civilne strukture je postala ena izmed glavnih prednostnih nalog sodobnih oboroženih sil. Takšni napadi lahko ogrozijo nacionalno varnost, vojaške operacije in infrastrukturo, nujno za delovanje države, med katero sodijo tudi oskrbovalne poti, skladišča in transportna vozlišča, od katerih je odvisna tako civilna kot vojaška logistika. Vojaške organizacije morajo biti zato

sposobne grožnje zaznati in se nanje odzvati, da zaščitijo državne skrivnosti in ohranijo operativne zmožnosti. Kibernetska obramba je sestavni del vojaške pripravljenosti, zato morajo biti pripadniki usposobljeni in opremljeni za obrambo pred kibernetskimi grožnjami, kar vključuje razvoj in vzdrževanje naprednih obrambnih sistemov. Poleg obrambnih dejavnosti se oborožene sile ukvarjajo tudi s kibernetskim vojskovanjem, ki lahko vključuje izvajanje ofenzivnih kibernetskih operacij kot del strategije odvračanja ali kot odgovor na agresijo. Vojaške enote sodelujejo z zavezniki in mednarodnimi partnerji ter si izmenjujejo informacije in usklajujejo odzive na kibernetske grožnje, kar je bistveno za oblikovanje globalnega odgovora na kibernetsko vojskovanje. Kibernetska obramba pri tem deluje v okviru nacionalnega in mednarodnega prava, vključno s pravili oboroženih spopadov in etičnimi normami (povzeto po Plevnik in Ščavničar, 2026).

V literaturi najdemo vrsto opredelitev kibernetske obrambe, ki se bolj ali manj osredotočajo na obrambne procese v kibernetskem prostoru. McCargo (2020) jo povezuje z akterji groženj in varnostjo sistema, pri čemer izpostavi, da se uporablja poseben nabor orodij, ter jo poveže z vojaško organizacijo. Drugačen pogled zajema obrambne mehanizme informacijskih sistemov, ki vključujejo odzivanje in ukrepe za zaščito kritične infrastrukture ter zagotavljanje informacij za organizacije in vladne subjekte, pri čemer je poudarek na preprečevanju, odkrivanju in pravočasnem odzivanju na napade ali grožnje, da ne pride do posegov v infrastrukturo ali informacije (Rouse, 2024). Ožja opredelitev zajema zgolj zmožnost odzivanja na kibernetske napade (Walia, 2024). Razširjeno se izraz nanaša na sposobnost preprečevanja kibernetskih napadov, ki bi okužili informacijski sistem, in vključuje aktivne ukrepe za predvidevanje kibernetskih dejanj nasprotnika ter preprečevanje vdorov (CyberTalk.org, 2024). Vsem strategijam in taktikam kibernetske obrambe je skupen cilj preprečevanje, onemogočanje in odzivanje na kibernetske grožnje. Aiyanyo idr. (2020) kibernetsko obrambo opredelijo kot boj proti zlonamernim grožnjam, katerega cilj je s sistemi kibernetske obrambe ohraniti zasebnost, celovitost in dostopnost informacij pred notranjimi in zunanjimi grožnjami. NIST jo opredeli z ukrepi za zaščito pred nepooblaščenimi dejavnostmi v računalniških omrežjih, ki vključujejo spremljanje, odkrivanje, analizo, na primer analizo trendov in vzorcev, ter dejavnosti odzivanja in obnove (Paulsen in Byers, 2019). Opredelitev ENISE (2017) se nanaša na različne obrambne mehanizme, ki se lahko uporabijo za ublažitev kibernetskih napadov ali odziv nanje. Nato kibernetsko obrambo opredeli kot način doseganja in izvajanja obrambnih ukrepov za preprečevanje kibernetskih napadov in ublažitev njihovih učinkov, s ciljem ohraniti in obnoviti varnost komunikacijskih, informacijskih ali drugih elektronskih sistemov oziroma informacij, ki so v njih shranjene, obdelane ali prenesene (NATO, 2014a). V slovenski pravni red je opredelitev vnesel Zakon o informacijski varnosti, po katerem je kibernetska obramba celota ukrepov in dejavnosti države, s katerimi se odvrača,

onemogoča, preprečuje ali odbija kibernetske napade v informacijskem okolju (ZInfV, 2018). Novi Zakon o informacijski varnosti opredelitev nadgrajuje, saj kibernetsko obrambo določa kot celoto ukrepov, dejavnosti in zmogljivosti za preprečevanje kibernetskih groženj in incidentov ter ublažitev njihovih vplivov, ki vključuje vse tri plasti kibernetskega prostora, družbeno, logično tehnično in fizično (ZInfV-1, 2025).

Iz navedenih opredelitev izpeljemo delovno opredelitev, ki jo bomo uporabljali za enotno razumevanje. Kibernetska obramba zajema tehnične, organizacijske in druge vojaške aktivnosti za obrambo države v kibernetskem prostoru. Delovna opredelitev preprečuje napačne razlage in nesporazume.

2.2.5 Pojmovna zmeda

Pojmovna zmeda na področju varovanja kibernetskega prostora lahko močno vpliva na razumevanje in razvoj ukrepov za kibernetsko varnost. Zato je pomembno, da strokovnjaki, vlade in mednarodne organizacije združijo napore pri vzpostavljanju enotnejših, jasnejših in splošno sprejetih definicij ter standardov na področju kibernetske varnosti. Usklajevanje in sodelovanje med deležniki sta temelj učinkovite zaščite kibernetskega prostora pred naraščajočimi grožnjami (povzeto po Plevnik in Ščavničar, 2026).

V literaturi je na pojmovnem področju varovanja kibernetskega prostora opazna zmeda, ki predvsem zmanjšuje operativno vrednost pojmov. Vzrok zanjo je dejstvo, da so opredelitve, še bolj pa njihove interpretacije, nastajale v različnih časovnih obdobjih in sledile razvoju področja.

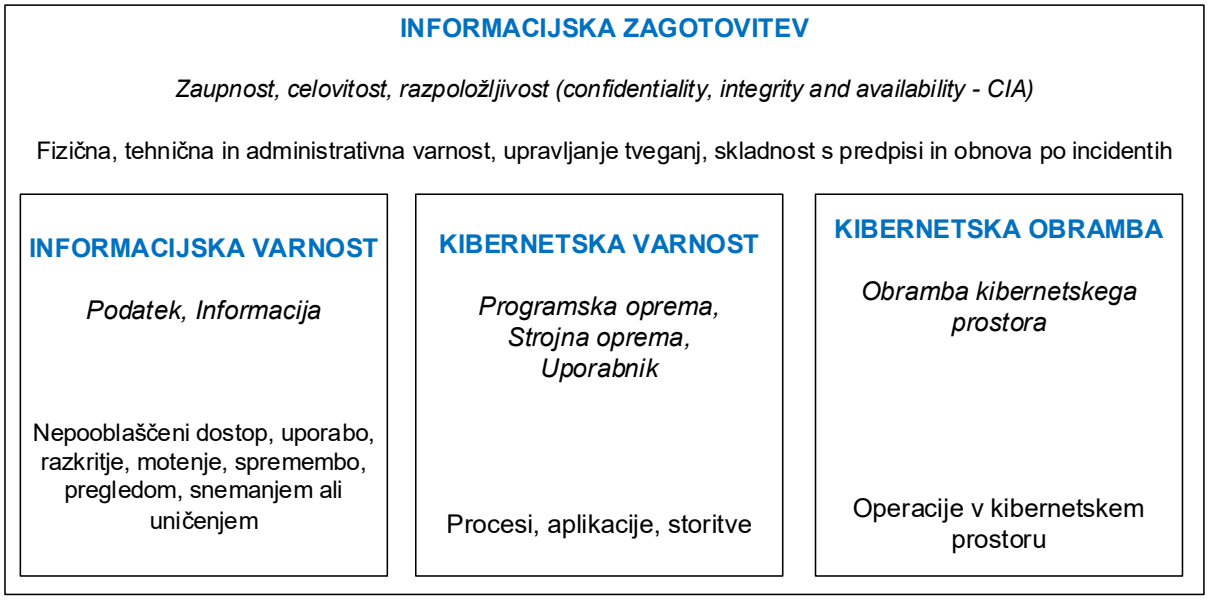
Različne opredelitve temeljnih varnostnih pojmov, kot so informacijska zagotovitev, informacijska varnost, kibernetska varnost in kibernetska obramba, pomembno vplivajo tudi na delovanje logističnih organizacij. Povzročijo lahko zmedo pri oblikovanju varnostne strategije in internih politik, vplivajo na usposabljanje in pripravljenost zaposlenih, otežujejo sodelovanje in koordinacijo s partnerji v oskrbovalni verigi ter privedejo do neusklajenosti pri izbiri in uvajanju tehničnih rešitev, na primer pri varovanju skladiščnih in transportnih sistemov. Neenotne opredelitve ustvarjajo tudi izzive pri zagotavljanju skladnosti z zakonodajnimi in etičnimi zahtevami, kar je občutljivo zlasti za podjetja, ki poslujejo čezmejno in morajo hkrati upoštevati več pravnih redov. Za učinkovito naslavljanje kibernetskih groženj je zato bistveno, da logistične organizacije in njihovi partnerji razvijejo usklajene opredelitve, ki omogočajo jasno strategijo, boljše usposabljanje, učinkovito sodelovanje med organizacijami, dosledno uvajanje tehničnih

rešitev ter upoštevanje pravnih in etičnih standardov. To ne izboljša samo varnosti posamezne organizacije, ampak zagotavlja tudi, da oskrbovalne verige ostanejo prilagodljive in odzivne v hitro spreminjajočem se kibernetskem okolju.

2.2.6 Razmerja med pojmi

Informacijska zagotovitev, informacijska varnost, kibernetska varnost in kibernetska obramba so osrednja področja sodobnega digitalnega okolja, ki zahteva celovit pristop k zaščiti informacij, omrežij in sistemov. Različni standardi, zakoni in definicije podajajo koncepte in ukrepe, namenjene ohranjanju razpoložljivosti, celovitosti, verodostojnosti, zaupnosti in nepreklicnosti informacij.

Razmerja med informacijsko varnostjo, kibernetsko varnostjo in kibernetsko obrambo lahko opredelimo kot medsebojno povezana in dopolnjujoča se (glej Sliko 6). Informacijska varnost zajema aktivnosti za zaščito podatkov in informacij pred nepooblaščenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem, pregledovanjem, snemanjem ali uničenjem, vključuje pa tudi fizično in kadrovsko varnost. Kibernetska varnost k temu doda programsko opremo, strojno opremo in uporabnika ter zajema procese, aplikacije in storitve za zaščito uporabnikov, strojne opreme, programske opreme, storitev in vseh informacij v kibernetskem prostoru. Kibernetska obramba je še ožja, saj obravnava obrambo kibernetskega prostora in bojevanje v njem ter se osredotoča na strategije, tehnike in postopke za obrambo računalniških sistemov, omrežij in podatkov pred kibernetskimi napadi, pri čemer zajema tako pasivne kot aktivne obrambne ukrepe za preprečevanje, zaznavanje in odzivanje nanje. Informacijska zagotovitev kot najširši pojem zajame vsa tri področja in zagotavlja zaupnost, celovitost in razpoložljivost informacij (angl. *Confidentiality, Integrity, Availability*). Razumevanje teh razmerij je koristno tudi v logistični praksi, saj pokaže, da varovanje oskrbovalne verige ne pomeni samo tehnične zaščite sistemov, temveč tudi varovanje dokumentov, ljudi in prostorov ter jasno razdelitev odgovornosti med informatiki in drugimi službami (povzeto po Plevnik in Ščavničar, 2026).



Slika 7: Razmerja med pojmi varovanja kibernetskega prostora.
Vir: lasten.

Zaradi nenehnih sprememb in tehnološkega napredka je nujno, da organizacije, institucije in države svoje strategije informacijske zagotovitve, informacijske varnosti, kibernetske varnosti in kibernetske obrambe stalno prilagajajo in razvijajo ter tako ostajajo korak pred vse kompleksnejšimi kibernetskimi grožnjami. To velja tudi za logistične sisteme, ki se med digitalizacijo oskrbovalnih verig srečujejo z vedno novimi ranljivostmi.

2.3 Informacijsko-kibernetske grožnje

Informacijske in kibernetske grožnje sodijo med tiste grožnje, ki lahko v sodobnem varnostnem okolju bistveno zmanjšajo kakovost družbenega življenja ali ga celo ohromijo. Zaradi takšnega pomena se uvrščajo med najpomembnejše dejavnike varnosti na nacionalni, mednarodni in globalni ravni. Enako neposredno ogrožajo gospodarstvo, saj lahko ustavijo proizvodnjo, promet in oskrbo, torej procese, ki jih povezuje logistika. V okolju obstajajo zelo raznolike vrste teh groženj, od enostavnih do kompleksnih. Zaradi njihove razsežnosti jih bomo najprej opredelili v splošnem smislu in prikazali skozi tipologijo, pozornost pa bomo namenili tudi modelu, ki kibernetske grožnje opredeljuje celostno. Poleg tega bomo v podpoglavju grožnje med seboj primerjali in podali predloge za njihovo boljšo in jasnejšo opredelitev (povzeto po Plevnik in Ščavničar, 2026).

2.3.1 Opredelitev pojma kibernetske grožnje

Opredelitev pojma kibernetskih groženj je temelj za oblikovanje celostnih strategij kibernetske varnosti. Organizacijam omogoča boljše razumevanje in obvladovanje tveganj, izboljšuje skladnost z zakonskimi zahtevami, usmerja razvoj tehničnih in organizacijskih zaščitnih ukrepov ter spodbuja kulturo varnosti med zaposlenimi. Prav tako olajšuje sodelovanje med organizacijami in državami ter izboljšuje odzivanje na varnostne incidente. Jasno določene kibernetske grožnje zagotavljajo, da so varnostni protokoli in postopki prilagojeni specifičnim nevarnostim, s katerimi se organizacija sooča, kar vodi k odpornejšemu in bolje zaščitenemu informacijskemu okolju. Za logistično podjetje to pomeni, da varnostnih ukrepov ne oblikuje na pamet, temveč glede na grožnje, ki dejansko ogrožajo njegova skladišča, vozila in izmenjavo podatkov s partnerji (povzeto po Plevnik in Ščavničar, 2026).

V literaturi najdemo vrsto opredelitev kibernetskih groženj, ki se osredotočajo na potencialno škodljive ali nevarne dejavnosti v kibernetskem prostoru. Kibernetsko grožnjo lahko opredelimo neformalno in formalno (Mateski idr., 2021). Neformalno je opredeljena kot oseba ali organizacija, ki namerava povzročiti škodo. Formalno pa je zlonamerni akter, organizacija ali posameznik, ki ima določen politični, družbeni ali osebni cilj ter določeno raven zmogljivosti in namere, da nasprotuje uveljavljeni vladi, zasebni organizaciji ali sprejeti družbeni normi. Najosnovnejša opredelitev izhaja iz skupnega prostora, v katerem se prepletajo ljudje, internet in računalniki, zato je grožnja lahko poštena napaka ali zlonameren udarec (Ulsch, 2014). Ta opredelitev poudarja interakcijo med človekom in kibernetskim prostorom ter ugotavlja, da te interakcije segajo od nenamernih napak do namernih škodljivih dejanj. Oxfordski slovar kibernetske grožnje opredeli kot možnost, da bo nekdo poskušal poškodovati ali uničiti računalniško omrežje, računalniški sistem ali spletno mesto tako, da bo na skrivaj in brez dovoljenja spreminjal podatke (Oxford University Press, 2023). ISO/IEC (2020) v publikaciji ISO/IEC TS 27100:2020 kibernetske grožnje opredeli vzročno in posledično kot neželen kibernetski varnostni incident, ki lahko povzroči škodo sistemu, ljudem, družbi, organizaciji ali drugim subjektom v kibernetskem prostoru. NIST jih opredeli podrobneje in sistematično kot vsako okoliščino ali dogodek, ki bi lahko prek informacijskega sistema negativno vplival na organizacijske operacije, vključno s poslanstvom, funkcijami, podobo ali ugledom, na organizacijska sredstva ali na posameznike, in sicer z nepooblaščenim dostopom, uničenjem, razkritjem ali spreminjanjem informacij oziroma onemogočanjem storitev. Grožnja je tudi možnost, da njen vir uspešno izkoristi določeno ranljivost informacijskega sistema (Paulsen in Byers, 2019). V slovenskem pravnem redu je opredelitev kibernetskih groženj del razlage izrazov v Zakonu o informacijski varnosti, ki kibernetsko grožnjo

opredeli kot možnost zlonamernega poskusa poškodovanja ali prekinitve računalniškega omrežja, sistema, storitev in podatkov (ZInfV, 2018). Novi zakon jo opredeljuje širše, kot vsako potencialno okoliščino, dogodek ali dejanje, ki bi lahko poškodovalo, prekinilo ali drugače škodljivo vplivalo na omrežja in informacijske sisteme, uporabnike takih sistemov in druge osebe (ZInfV-1, 2025).

Iz navedenih opredelitev izpeljemo delovno opredelitev kibernetske grožnje. Glede na obravnavano literaturo jo lahko opredelimo kot možnost zlonamernega poskusa, dogodka ali okoliščine, ki lahko povzroči škodo ali prekinitev računalniškega omrežja, sistema, storitev, informacij ali podatkov. Vključuje lahko nepooblaščen dostop, uničenje, razkritje, spreminjanje informacij ali onemogočanje storitev, pa tudi možnost, da vir grožnje izkoristi ranljivosti informacijskega sistema. Te grožnje lahko negativno vplivajo na operacije organizacije, njena sredstva, poslanstvo, funkcije, podobo ali ugled, pa tudi na posameznike, družbo in širšo skupnost v kibernetskem prostoru. V logistiki mednje sodi tudi prekinitev informacijskega toka, ki ustavi naročanje, skladiščenje ali prevoz blaga. Delovna opredelitev omogoča enotno razumevanje pojma, kar je nujno za primerjavo in analizo groženj.

Dobra opredelitev pojma kibernetskih groženj omogoča boljšo pripravljenost in odzivnost ob kibernetskih incidentih, organizacijam in posameznikom pa pomaga razumeti vrsto in naravo potencialnih nevarnosti. To vodi v učinkovitejše načrtovanje varnostnih strategij, razvoj ustreznih obrambnih mehanizmov in izobraževanje zaposlenih o varnostnih praksah. Jasno opredeljene kibernetske grožnje poleg tega prispevajo k boljšemu mednarodnemu sodelovanju in kakovostnejši zakonodaji na področju varnosti v kibernetskem prostoru.

2.3.2 Model kibernetskih groženj

Model kibernetskih groženj omogoča učinkovito izvajanje kibernetske varnosti. Organizacijam in vladnim agencijam daje možnost, da potencialne varnostne grožnje sistematično prepoznajo, ocenijo, primerjajo in se nanje odzovejo po standardiziranem modelu. Z njegovo uporabo se oblikujejo strategije za preprečevanje, zaznavanje in odzivanje na različne kibernetske incidente, kar omogoča boljše dodeljevanje virov, usmerjeno usposabljanje zaposlenih in razvoj učinkovitih obrambnih mehanizmov. V logistiki, kjer so varnostni proračuni običajno omejeni, tak model pomaga presoditi, katere grožnje najbolj ogrožajo delovanje oskrbovalne verige in kam je zato najprej treba usmeriti sredstva. Modeliranje kibernetskih groženj spodbuja tudi sodelovanje med organizacijami in državami ter zagotavlja, da so varnostni ukrepi skladni z zakonodajnimi in regulativnimi

zahtevami. Jasen model groženj je poleg tega temelj za razvoj učinkovitih programov izobraževanja in usposabljanja, s katerimi zaposleni prepoznajo kibernetske napade in se nanje ustrezno odzovejo. Tako se zagotavlja trdna obramba pred grožnjami, ki se nenehno spreminjajo in razvijajo, hkrati pa se ohranja zaupanje v digitalno infrastrukturo in tehnologije (povzeto po Plevnik in Ščavničar, 2026).

Svete (2007) na področju kibernetskih groženj ugotavlja, da so omrežja v sodobnih družbah postala referenčni objekt, na katerega se varnost nanaša. Razlog je vse večji vpliv omrežnih informacijskih tehnologij na naše ustvarjanje, delovanje in bivanje v državi in družbi. Pojavila se je nova oblika varnostne predstave, usmerjena v zavarovanje omrežja pred razpadom, izgubo, krajo ali uničenjem podatkov ter prekinitvijo informacijskih tokov. Ta ima dve dimenziji. Prva se nanaša na zaščito neokrnjenosti podatkov in njihovega pretoka, torej na notranjo omrežno varnost oziroma zanesljivo delovanje informacijske infrastrukture. Druga se nanaša na varnost informacijskih tokov med ponudniki storitev in uporabniki, torej na omrežno varnost, usmerjeno v zunanje okolje omrežne organizacije. Takšno razlikovanje je blizu logistični praksi, saj mora podjetje ločeno obravnavati varnost svojih notranjih sistemov in varnost izmenjave podatkov s strankami, prevozniki in dobavitelji. Vire ogrožanja Svete (2007) razdeli v dve skupini, pri čemer prva opisuje fizično ogrožanje informacijske varnosti, druga pa uporabniško ogrožanje (glej Tabelo 1).

Tabela 48: Viri ogrožanja informacijske varnosti.

Informacijska zagotovitev	Višja sila	Potres, nevihte, poplave, strele, požar, visoka temperatura, visoka vlažnost, onesnaženost, radarsko sevanje, akustično sevanje, elektromagnetno sevanje v obe smeri, nestabilnost napajanja z električno energijo, izredne razmere, vojno stanje
	Pomanjkljivosti strojne in programske opreme	Izpad sistema, tehnične napake na osrednji enoti - strežniku, tehnične napake na odjemalcih, logične napake v strežnih programih, logične napake v aplikativni opremi
Družbeno in kulturno ogrožanje - (zlo) uporaba kot grožnja	Človeški dejavnik (nenamernost)	Slaba organizacija, nedisciplina, nemarnost, nestrokovnost, monotonost, utrujenost
	Človeški dejavnik (namernost)	Kraje, prevare, poneverbe, ponarejanje, izsiljevanje, grožnje, kršenje zasebnosti, sabotaže, sporočanje zaupnih podatkov, vohunjenje, pornografija, propaganda, vandalizem (*crackerji*), terorizem, hekerji, izdelava ter distribucija virusov, piratstvo na področju programske opreme, napadi DoS

Vir: Svete, 2007.

Tabela 49: Človeški indikatorji ogrožanja informacijske varnosti glede na namen in uporabljena sredstva.

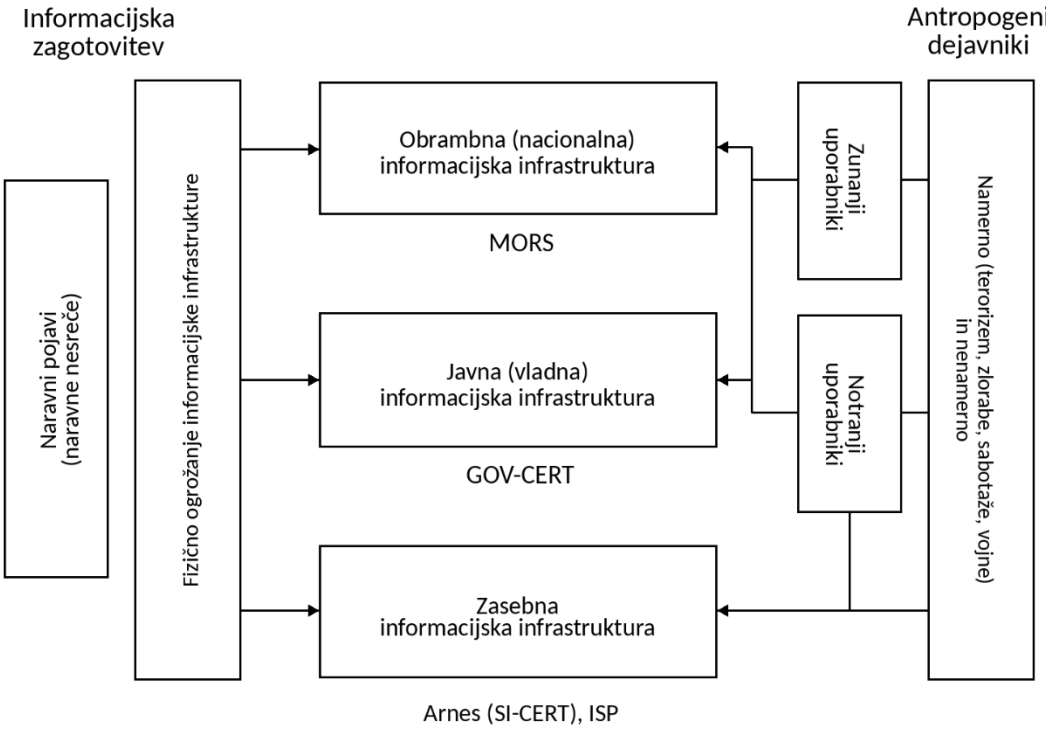
Človeška ogrožanja (viri)	Namen (motivacija)	Metode, načini delovanja
Hekerji, krekerji	Izziv, lasten ego, uporništvo	*Hacking*, sistemski vdori, neavtorizirani vstop v sistem
Računalniški kriminal	Uničevanje informacij Pridobitništvo (Finančno) neavtorizirano spreminjanje podatkov Nelegalno razkrivanje informacij	Računalniški kriminal Prevare Informacijsko podkupovanje "*Spoofing*" Sistemski vdor
Terorizem	Izsiljevanje Uničenje podatkov Izkoriščanje Maščevanje	Informacijsko bojevanje Sistemski napad - *DoS* Vdori v sisteme Nepooblaščeno spreminjanje sistemov
Industrijsko vohunjenje (družbe, tuje vlade, drugi vladni interesi)	Konkurenčna prednost Ekonomsko vohunjenje	Ekonomsko izkoriščanje Kraja podatkov, informacij Vdori oziroma kršitve zasebnosti Vdori v sistem Nepooblaščeni dostopi v sistem
Insiderji oziroma zaposleni (slabo izobraženi, nepazljivi, nepošteni, zahrbtni, odpuščeni)	Radovednost Ego Obveščevalna dejavnost Finančna korist Maščevanje Nenamerne napake pri vnosu podatkov Programske napake	Napad na zaposlene Izsiljevanje Brskanje po zasebnih informacijah Zlorabe računalnikov Prevare in kraje Informacijsko podkupovanje Vnos ponarejenih, uničenih podatkov Prisluškovanje Zahrbtna koda (virusi, logične bombe, trojanski konji) Prodaja osebnih informacij Sistemske napake oziroma hrošči Vdori v sisteme Sistemske sabotaže Nepooblaščeni vstopi v sistem

Vir: Dunn in Wigert, 2004.

Dunn in Wigert (2004) po drugi strani predstavljata različne vrste groženj v kibernetskem prostoru ter njihove motive in metode delovanja (glej Tabelo 2). Hekerje in krekerje motivirajo izzivi, lastni ego in uporništvo, pri tem pa uporabljajo tehnike, kot sta vdiranje (angl. *Hacking*) in sistemski vdori. Računalniški kriminal zajema uničevanje informacij in pridobitništvo s prevarami ter informacijskim podkupovanjem. Terorizem vključuje izsiljevanje, uničenje podatkov, izkoriščanje in maščevanje z metodami, kot sta informacijsko bojevanje in sistemski napadi. Industrijsko vohunjenje in vohunjenje tujih vlad za doseganje konkurenčne prednosti vključujeta krajo podatkov in vdore v zasebnost, kar v logistiki pomeni tudi krajo poslovno občutljivih podatkov o cenah, strankah in blagovnih tokovih. Notranji akterji (angl. *Insiders*), na primer zaposleni, lahko delujejo iz radovednosti, finančnih motivov ali maščevanja, njihove metode pa vključujejo napade na druge zaposlene, zlorabe računalnikov in sistemske sabotaže. Prav notranji akterji so v

skladiščih in transportnih službah pogosto spregledana ranljivost, ker imajo neposreden dostop do sistemov in blaga. Takšen pregled omogoča boljše razumevanje in naslavljanje raznolikih groženj, ki vplivajo na kibernetsko varnost.

Ocenjevanje informacijske dimenzije ogrožanja nacionalne varnosti povzemamo po Svetetu (2007), ki je informacijsko področje razdelil na tri glavne komponente, na katere se nanašajo varnost in mehanizmi za njeno zagotavljanje (glej Sliko 7). Te komponente so ogrožanje obrambne (nacionalne) informacijske infrastrukture, ogrožanje javne (vladne) informacijske infrastrukture in ogrožanje zasebne informacijske infrastrukture. Povzročitev nedelovanja prve pomeni neposreden napad na enega glavnih instrumentov za zagotavljanje nacionalne varnosti. Ogrožanje druge je izziv za nacionalno varnost, saj je prizadeta informacijska infrastruktura, na kateri temelji delovanje elektronske uprave. Informacijsko razvite države zato ustanavljajo službe za preprečevanje in analizo teh varnostnih incidentov (angl. *Computer Emergency Response Team*). V tretjem primeru gre za posameznike in pravne osebe, kamor sodi tudi večina logističnih podjetij z lastnimi skladiščnimi, transportnimi in poslovnimi sistemi. Pri preprečevanju teh ogrožanj imajo osrednjo vlogo ponudniki dostopa do storitev (angl. *Internet Service Provider*).



Slika 8: Ocenjevanje informacijske dimenzije ogrožanja nacionalne varnosti.
Vir: Svete, 2007.

V prvem primeru gre za zelo dobro sistemsko razdelitev po tehnični plati, in sicer na pet razredov ogrožanja omrežja ter na opredelitev fizične grožnje inštalaciji. V drugem primeru Svete postavi model ogrožanja informacijske varnosti v Sloveniji in vire ogrožanja razdeli v dve skupini, na fizično in uporabniško ogrožanje. Predstavljeni model bo v nadaljevanju osnova za ocenjevanje in primerjavo kibernetskih groženj v obravnavanih dokumentih.

2.3.3 Kibernetske grožnje

Kibernetske grožnje so med najbolj perečimi sodobnimi varnostnimi izzivi, saj z različnimi napadi neprestano ogrožajo zasebne, poslovne in vladne entitete. Napadi segajo od kraje identitete in finančnih prevar do sabotaž kritične infrastrukture in državnega vohunjenja. Vseprisotna in dinamična narava teh groženj zahteva stalno budnost, napredek varnostnih tehnologij, medsektorsko sodelovanje in globalno koordinacijo, da se zaščitijo najpomembnejši informacijski viri, ohrani zasebnost in zagotovi mednarodna stabilnost. Kibernetske grožnje so zato postale pomembna sestavina strateškega načrtovanja vsake države in organizacije, tudi logističnih podjetij, pri obrambi pred nepredvidljivimi in kompleksnimi kibernetskimi napadi pa sta odločilni odzivnost in prilagodljivost. V nadaljevanju podajamo izbrane opredelitve kibernetskih groženj, ki jih bomo podrobneje analizirali glede na vire ogrožanja in primerjali z namenom ugotovitve različnih skupin kibernetskih groženj po Svetetovem (2007) modelu (povzeto po Plevnik in Ščavničar, 2026).

Strategija kibernetske varnosti kibernetske grožnje opredeljuje kot dejavnosti, ki ogrožajo integriteto, zaupnost in razpoložljivost informacij ter informacijskih sistemov (Vlada RS, 2016a). Grožnje lahko izvirajo iz različnih virov, vključno s kibernetskim kriminalom, vohunjenjem in terorizmom. Strategija poudarja pomen celovitega pristopa h kibernetski varnosti, ki vključuje strategije preprečevanja, zaznavanja in odzivanja, ter izpostavlja potrebo po sodelovanju med deležniki, torej vlado, zasebnim sektorjem in mednarodnimi partnerji, za učinkovito upravljanje in zmanjševanje teh groženj.

Resolucija o strategiji nacionalne varnosti Republike Slovenije kibernetske grožnje opredeli podrobno (ReSNV-2, 2019). Mednje uvršča hibridne grožnje, informacijske in kibernetske grožnje, obveščevalno dejavnost tujih akterjev in druge. Poseben poudarek namenja značilnostim kibernetskega okolja, kot so globalna narava, asimetričnost, horizontalnost in težavna določljivost dejanskega vira grožnje. Grožnje obsegajo kibernetske napade, spletno vohunjenje, krajo intelektualne lastnine, širjenje dezinformacij, kibernetski kriminal in terorizem. Poudarjena je ranljivost sodobne družbe

zaradi odvisnosti od informacijskih tehnologij in sistemov, ki je v oskrbovalnih verigah še posebej izrazita.

Zakon o informacijski varnosti določa, da CSIRT državnim organom za potrebe pravočasnega odzivanja na kibernetske grožnje in preprečevanja škodljivih posledic odredi ustrezne, nujne in sorazmerne ukrepe, ki jih morajo ti nemudoma oziroma v določenem roku izvesti v svojem informacijskem in komunikacijskem sistemu (ZInfV, 2018).

ENISA (2022) vsako leto pripravi pregled groženj (angl. *Threat Landscape*). Za preteklo leto je zajemal izsiljevalsko programsko opremo, zlonamerno programsko opremo, grožnje socialnega inženiringa, grožnje za podatke, grožnje zoper razpoložljivost v obliki zavrnitve storitve, internetne grožnje, dezinformacije in napačne informacije ter napade na dobavno verigo, ki neposredno zadevajo logistične organizacije in njihove partnerje. Med vzroki za grožnje ENISA izpostavi konflikt med Ukrajino in Rusijo, vse močnejši vpliv geopolitike na kibernetske operacije, destruktivne napade kot pomembno sestavino delovanja državnih akterjev, nov val haktivizma in dezinformacije kot orodje kibernetskega vojskovanja. Kot akterje groženj opredeli državno sponzorirane akterje, kibernetski kriminal, najete hekerje in haktiviste.

Nacionalni načrt odzivanja na kibernetske incidente (v nadaljevanju NOKI) opredeli podrobno taksonomijo kibernetskih incidentov in jih razdeli na žaljivo oziroma zlonamerno vsebino, zlonamerno kodo, zbiranje informacij, poskuse vdora, vdore, razpoložljivost, varnost informacijskih virov, goljufije, ranljivost, drugo in test (Vlada RS, 2021). Klasifikacija je nastala na osnovi klasifikacije Evropske agencije za kibernetsko varnost ter je dopolnjena s taksonomijo Nata in taksonomijo SI-CERT.

SI-CERT v letnem poročilu kibernetske incidente predstavi po taksonomiji NOKI (ARNES, 2023a). Med opažanji ugotavlja, da je kibernetsko vojskovanje zaradi vojne v Ukrajini prestopilo geografske meje. Bolj razširjen je pojav dezinformacij in propagande, prisotni pa sta tudi izraba vojnega stanja za izvedbo spletnih goljufij in rast napadov onemogočanja, ki lahko prizadenejo tudi spletne portale za naročanje in sledenje pošiljkam.

EU (2022) v strateškem kompasu opredeli, da državni in nedržavni akterji uporabljajo hibridne strategije, kibernetske napade, dezinformacijske kampanje, neposredno vmešavanje v volitve in politične procese, ekonomsko prisilo in instrumentalizacijo nedovoljenih migracijskih tokov.

ENISA (2023c) je pripravila tudi prepoznavanje nastajajočih groženj in izzivov kibernetske varnosti do leta 2030. Te zajemajo ogroženost dobavne verige zaradi odvisnosti od programske opreme, napredne kampanje dezinformiranja in vplivanja, porast avtoritarnosti digitalnega nadzora in izgubo zasebnosti, človeške napake in izkoriščene podedovane sisteme v kiberfizičnih ekosistemih, ciljno usmerjene napade, na primer z izsiljevalsko programsko opremo, pametne naprave, okrepljene s podatki, pomanjkljivo analizo in nadzor vesoljske infrastrukture in objektov, porast naprednih hibridnih groženj, pomanjkanje spretnosti, čezmejne ponudnike storitev KIS kot enotno točko odpovedi ter zlorabo umetne inteligence. Velik del teh groženj neposredno zadeva digitalizirano logistiko, od pametnih naprav v skladiščih do satelitskega sledenja prevozov.

Obrambna strategija Republike Slovenije, sprejeta leta 2024, med vire ogrožanja nacionalne varnosti uvršča kibernetske grožnje ter zlorabo informacijskih tehnologij in sistemov, na katere se obrambni sistem odziva samostojno ali v sodelovanju z drugimi podsistemi nacionalne varnosti, Natom in EU. Delovanje v kibernetskem prostoru opredeljuje kot novo operativno domeno poleg kopnega, zraka in morja, kibernetsko varnost in obrambo pa uvršča med podporne funkcije obrambnega sistema. Pripravljenost in vzdržljivost obrambnega sistema bosta podprti z nadgradnjo komunikacijskih in informacijskih sistemov ter kibernetske varnosti, v okviru Nata in EU pa bo Slovenija krepila pripravljenost za odzivanje na kibernetske grožnje (Vlada RS, 2024a).

Vojaška strategija Republike Slovenije, sprejeta leta 2024, opredeljuje, da se kibernetski vdori pojavljajo pod pragom vojne in da se vojaško delovanje seli v kibernetski prostor (Vlada RS, 2024b). Med vojaške grožnje so uvrščeni tudi kibernetski napadi. Ob poslabšanju mednarodnih ali regionalnih političnih in varnostnih razmer bomo izpostavljeni napadom v kibernetskem in informacijskem prostoru. Slovenska vojska bo prispevala h kibernetski varnosti države, kibernetska obramba pa podpira, dopolnjuje in krepi zmogljivosti in izvajanje vojaške obrambe države.

Furlan (2021) kibernetske grožnje predstavi na primeru gruzijske vojaške strategije in jih uvrsti med tveganja, grožnje in izzive koncepta nacionalne varnosti. Omeni jih tudi ob izdelavi Resolucije o strategiji nacionalne varnosti iz leta 2019, ko je javna razprava v akademskem okolju poudarila potrebo po usklajenem odzivanju na kibernetske grožnje.

Kibernetske grožnje so torej eden najbolj perečih varnostnih izzivov sodobnega časa, ki na raznolike načine nenehno ogroža zasebne, poslovne in vladne entitete. Ker segajo od kraje identitete in finančnih prevar do sabotaž kritične infrastrukture in državnega vohunjenja, zahtevajo nenehno budnost, napredek varnostnih tehnologij, medsektorsko

sodelovanje in globalno koordinacijo. Postale so pomembna sestavina strateškega načrtovanja organizacij in držav, pri obrambi pred nepredvidljivimi in kompleksnimi napadi pa štejeta predvsem odzivnost in prilagodljivost. Dinamična narava teh groženj poudarja potrebo po celovitem pristopu h kibernetski varnosti, ki vključuje strategije preprečevanja, zaznavanja in odzivanja ter sodelovanje med deležniki za učinkovito upravljanje in zmanjševanje groženj.

V nadaljevanju bomo na podlagi zgornjih opredelitev izvedli primerjavo, s katero bomo natančneje opredelili razmerja med kibernetskimi grožnjami v obravnavanih dokumentih.

2.3.4 Primerjava kibernetskih groženj

Skladno z opredelitvami, ki jih ponujajo različni avtorji in institucije, se kibernetske grožnje nanašajo na različne oblike nevarnosti, ki lahko prizadenejo informacijska omrežja, sisteme in podatke. Skupna točka vseh opredelitev sta nepooblaščen dostop do informacij in možnost negativnega vpliva na delovanje organizacij, posameznikov ali družbe kot celote. Zavedanje teh groženj je temelj učinkovite kibernetske varnosti, saj omogoča razvoj preventivnih ukrepov in strategij za obvladovanje morebitnih incidentov. S tem se kaže potreba po stalnem prilagajanju pristopov k varnosti informacijskih sistemov, da se lahko organizacije, med njimi tudi logistične, učinkovito odzivajo na nenehno spreminjajoče se kibernetske grožnje.

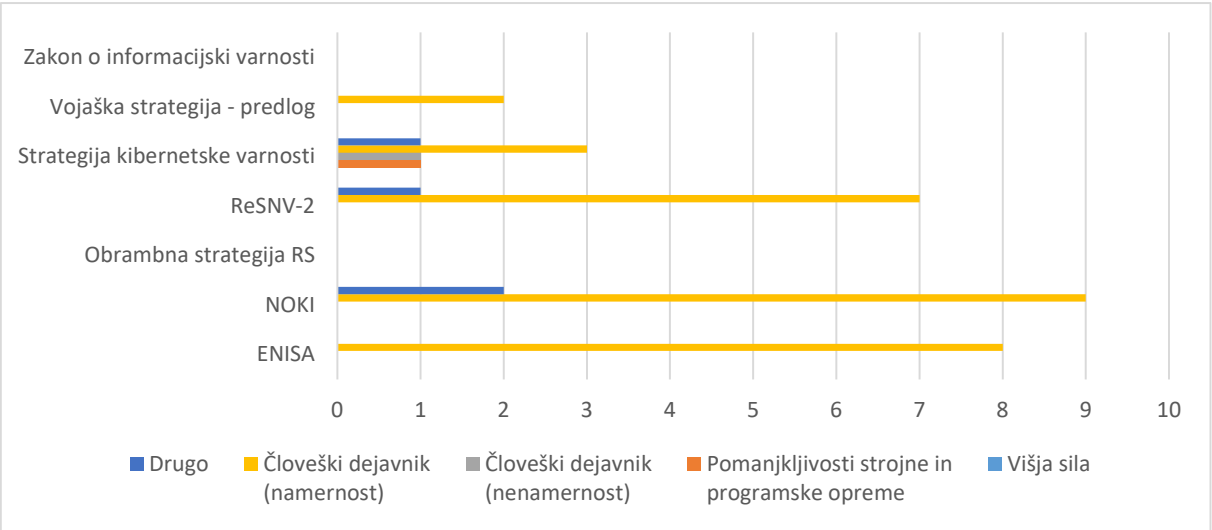
Primerjava kibernetskih groženj v obravnavanih dokumentih temelji na kvalitativni analizi, ki sta jo avtorja s programskim orodjem NVivo (različica 14) izvedla s kodiranjem besedil po Svetetovem (2007) modelu groženj (Plevnik in Ščavničar, 2026). Primerjava (glej Tabelo 3) pokaže, da večina kibernetskih groženj sodi v skupino namernih človeških dejavnikov. V skupini nenamernih dejavnikov je opredeljena le ena grožnja, prav tako ena v skupini pomanjkljivosti strojne opreme, štiri grožnje pa ne spadajo v nobeno od prvih štirih skupin. Obravnavani dokumenti torej pretežno opredeljujejo namerne človeške dejavnike, drugim skupinam groženj pa posebne pozornosti ne namenjajo. Za prakso je to pomembno opozorilo, saj v logistiki izpade pogosto povzročijo tudi nenamerne napake zaposlenih in odpovedi opreme, ne le napadi.

Tabela 50: Primerjava kibernetskih groženj.

	Višja sila	Pomanjkljivost strojne in programske opreme	Človeški dejavnik (nenamernost)	Človeški dejavnik (namernost)	Drugo
ENISA	0	0	0	8	0
NOKI	0	0	0	9	2
Obrambna strategija RS	0	0	0	0	0
ReSNV-2	0	0	0	7	1
Strategija kibernetske varnosti	0	1	1	3	1
Vojaška strategija	0	0	0	2	0
Zakon o informacijski varnosti	0	0	0	0	0

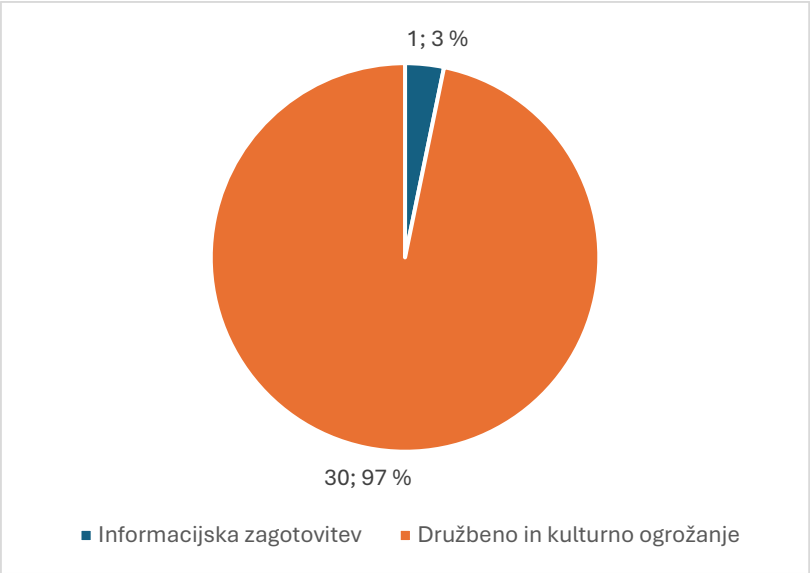
Vir: lasten.

Razmerje med različnimi dejavniki znotraj obravnavanih dokumentov (glej Graf 1) pokaže, da je največ groženj opredeljenih v NOKI, sledi resolucija, nato strategija. Zakon o informacijski varnosti, Vojaška strategija, Strategija kibernetske varnosti in Obrambna strategija Republike Slovenije kibernetske grožnje opredeljujejo pomanjkljivo. Ne zajamejo vseh dimenzij kibernetskih groženj, zanemarijo celoten sklop groženj znotraj informacijske zagotovitve ter ne opredelijo groženj zaradi višje sile in pomanjkljivosti strojne ter programske opreme. Prav te pa so v logistiki pogost vzrok motenj, saj lahko poplava, požar ali odpoved strežnika oskrbovalno verigo ustavi enako učinkovito kot kibernetski napad. Edino Strategija kibernetske varnosti opredeli vsaj po eno grožnjo iz vsakega sklopa, kar pa je glede na vrsto dokumenta še vedno premalo.



Graf 1: Primerjava kibernetskih groženj po obravnavanih dokumentih.
Vir: lasten.

Primerjava kibernetskih groženj med informacijsko zagotovitvijo in družbenim ogrožanjem (glej Graf 2) prikaže razmerje med tema kategorijama groženj. Velika večina opredeljenih groženj, kar 97 odstotkov, sodi v kategorijo družbenih in kulturnih ogrožanj, le 3 odstotki pa v skupino informacijske zagotovitve.



Graf 2: Primerjava kibernetskih groženj med informacijsko zagotovitvijo in družbenim ogrožanjem.
Vir: lasten.

Grafična analiza besedila (angl. *Word Art*) omogoča vizualno predstavitev najpogostejših besed s področja kibernetskih groženj v izbranih dokumentih (glej Sliko 8). Gre za grafični prikaz, v katerem so besede, ki se v besedilu pojavljajo pogosteje, izpisane večje, redkejše pa manjše. To omogoča hitro vizualno prepoznavanje najpomembnejših tem ali konceptov v besedilu in pomaga pri odkrivanju osrednjih tem, vizualnem povzemanju vsebine, analizi sentimenta, izboljšanju iskalnih izrazov ter pri izobraževalnih in pedagoških namenih. Grafična analiza temeljite analize vsebine in konteksta ne nadomešča, ampak služi kot dodatno orodje za hitro vizualizacijo in povzetek besedila.



Slika 9: Grafična analiza kibernetskih groženj v izbranih dokumentih.
Vir: lasten.

Skupna ugotovitev je, da kibernetske grožnje predstavljajo kompleksen in nenehno spreminjajoč se izziv za varnost in delovanje družbe. Pripravljeni moramo biti na širok spekter scenarijev, od vsakodnevnih incidentov do resnih kibernetskih napadov, ki imajo lahko globok vpliv na nacionalno varnost, gospodarstvo in družbo kot celoto. Posebej ranljive so oskrbovalne verige, saj se motnja pri enem členu hitro prenese na vse partnerje. Napad na skladiščni ali transportni sistem lahko ustavi dobavo blaga trgovinam, proizvodnji in zdravstvu, zato kibernetska varnost logističnih organizacij ni le njihova notranja zadeva, temveč pogoj za nemoteno oskrbo celotne družbe. Nujno je torej, da se prizadevanja za izboljšanje kibernetske varnosti nadaljujejo na vseh ravneh, od posameznikov prek podjetij do institucij, ter da se strategije, ukrepi in tehnologije nenehno prilagajajo, da ostanemo korak pred vedno naprednejšimi kibernetskimi grožnjami.

Univerzitetna založba
Univerze v Mariboru

3 Kibernetska varnost v NATU, EU in Sloveniji

V nadaljevanju bomo predstavili kibernetsko varnost v Natu in EU ter študija primera urejenosti kibernetske varnosti Slovenije.

3.1 Kibernetska varnost v NATU

Razvoj kibernetske varnosti v Natu prikazujemo strnjeno, skozi pregled deklaracij zasedanj vrha, kibernetske zaveze, politike minimalnih varnostnih ukrepov z zrelostnim modelom ter operacij v kibernetskem prostoru (povzeto po Plevnik in Ščavničar, 2026). Za bralca s področja logistike je ta pregled pomemben iz dveh razlogov. Natove usmeritve prek članstva zavezujejo tudi Slovenijo in njen obrambni sistem, odpornost zavezništva pa je neposredno odvisna od delovanja civilne infrastrukture, vključno s prometom in oskrbovalnimi verigami.

3.1.1 Razvoj skozi deklaracije vrhov in kibernetska zaveza

Analiza deklaracij zasedanj vrha od Rige leta 2006 do Vilne leta 2023 razkriva postopno in sistematično krepitev zavezništva pri odzivanju na kibernetske grožnje (glej Tabelo 4). V začetnem obdobju je bil poudarek na razvoju omrežnih zmogljivosti, izmenjavi informacij in zaščiti informacijskih sistemov (NATO, 2006). Sledila je uvedba zmogljivosti za odzivanje na računalniške incidente ter krepitev odkrivanja in odzivanja (NATO, 2010). Med letoma 2014 in 2016 je Nato kibernetsko obrambo vključil v temeljno nalogo kolektivne obrambe in kibernetski prostor priznal kot domeno delovanja, enakovredno kopnemu, morju in zraku (NATO, 2016a). Po letu 2018 sta bila v ospredju prilagajanje spreminjajočim se grožnjam ter sodelovanje z industrijo in akademskim svetom, zadnja

vrhova pa poudarjata večdomenske operacije, kibernetsko odpornost in nove podporne zmogljivosti (NATO, 2023). Stalnici celotnega obdobja sta zavezanost delovanju v skladu z mednarodnim pravom in vse večji pomen zaščite kritične infrastrukture. Razvoj se nadaljuje tudi po obravnavanem obdobju, na vrhu v Washingtonu leta 2024 je zavezništvo med drugim ustanovilo integrirani center za kibernetsko obrambo (NATO, 2024)

Tabela 51: Evolucija kibernetske varnosti Nata.

Vrh Nata	Razvoj kibernetske varnosti
Riga Summit Declaration, 2006	Ta vrh je bil začetek formalnega priznavanja kibernetske varnosti kot ključnega interesa za NATO. Poudarek je bil na prilagoditvi in razvoju omrežnih zmogljivosti za izboljšanje izmenjave informacij in zaščite ključnih informacijskih sistemov.
Bucharest Summit Declaration, 2008	Poudarek je bil na krepitvi ključnih informacijskih sistemov in uvedbi politike kibernetske obrambe. To je vključevalo razvoj struktur za njeno izvajanje in izmenjavo najboljših praks med državami članicami.
Strasbourg-Kehl Summit Declaration, 2009	NATO je okrepil svojo zavezanost k zaščiti komunikacijskih in informacijskih sistemov, ustanovil organ za kibernetsko obrambo in aktiviral Center odličnosti za kibernetsko obrambo v Estoniji.
Lisbon Summit Declaration, 2010	Opozorilo na hitro rast kibernetskih groženj in potrebo po celovitem pristopu k odkrivanju, ocenjevanju, preprečevanju, obrambi in okrevanju po kibernetskih napadih.
Chicago Summit Declaration, 2012	Poudarjena je bila rast števila in kompleksnosti kibernetskih napadov, ponovna potrditev zavez kibernetski obrambi in poudarek na integraciji kibernetske obrambe v strukture in postopke zavezništva.
Wales Summit Declaration, 2014	Potrjena je bila okrepljena politika kibernetske obrambe, poudarjena nedeljivost zavezniške varnosti in priznavanje kibernetskih napadov kot del kolektivne obrambe.
Warsaw Summit Communiqué, 2016	Kibernetski napadi so prepoznani kot jasen izziv za varnost zavezništva, s kibernetskim prostorom, ki se uradno priznava kot domena delovanja.
Brussels Summit Declaration, 2018	Opozorilo na povečanje kibernetskih groženj in potrebo po stalni prilagoditvi in izboljšanju nacionalnih kibernetskih obrambnih zmogljivosti.
Brussels Summit Communiqué, 2021	Poudarek na kompleksnosti in uničujoči naravi kibernetskih groženj, z večjo vlogo političnih posvetovanj in izboljšanega situacijskega zavedanja.
Madrid Summit Declaration, 2022	Osredotočenost na širše asimetrične grožnje, vključno s kibernetskimi, in potrebo po okrepitvi odvračanja in obrambe v vseh domenah.
Vilnius Summit Communiqué, 2023	Nadaljevanje dela na večdomenskih operacijah, poudarek na kibernetski odpornosti in sodelovanje z zasebnim sektorjem za izboljšanje kibernetske varnosti.

Vir: lasten, po NATO (2006, 2008, 2009, 2010, 2012, 2014b, 2016a, 2018b, 2021, 2022, 2023).

S kibernetsko zavezo z vrha v Varšavi leta 2016 so se članice zavezale, da bodo prednostno okrepile kibernetsko obrambo nacionalnih omrežij in infrastrukture (NATO, 2016b). Od držav se pričakuje razvoj zmogljivosti za obrambo nacionalnih infrastruktur, zagotavljanje ustreznih virov, krepitev sodelovanja med nacionalnimi deležniki, boljše razumevanje groženj z izmenjavo informacij in ocen, dvig znanja in ozaveščenosti vseh obrambnih deležnikov od osnovne kibernetske higiene naprej ter spodbujanje izobraževanja,

usposabljanja in urjenja. Napredek se spremlja letno na podlagi dogovorjenih kazalnikov. Te usmeritve se prek obrambnega sistema prenašajo tudi na podporne dejavnosti, med njimi na vojaško logistiko in njene civilne pogodbene partnerje.

3.1.2 Ukrepi za dvig kibernetske varnosti in operacije v kibernetskem prostoru

Nato je opredelil politiko minimalnih varnostnih ukrepov za zaščito svojih omrežij (NATO, 2019a), na njeni osnovi pa zrelostni model, ki zmogljivost varovanja KIS uvršča v sedem razredov, od neobstoječe do popolne (Gay idr., 2016) (glej Tabelo 5). Model se uporablja za izražanje ciljne in trenutno dosežene ravni varovanja ter za ugotavljanje primanjkljaja ali presežka zmogljivosti. Podoben pristop z zrelostnimi modeli uporabljajo tudi podjetja, zato je model uporaben zgled za samooceno varnosti v logističnih organizacijah. Za enotno obravnavo incidentov je Nato izdelal še taksonomijo kibernetskih incidentov z atributi, kot so vrsta incidenta, kategorizacija akterja, funkcionalni vpliv, vpliv na informacije in možnost obnove (NATO, 2019b).

Tabela 52: Zrelostni model.

Raven	Pomen	Rang	Opredelitev
0	Neobstoječe	0/10	Na tej ravni zmogljivost za vse namene ne obstaja.
1	Osnovno	2/10	Raven zmogljivosti se lahko na splošno šteje za začetno.
2	Postopno	4/10	Raven zmogljivosti se na splošno lahko šteje za podpovprečno.
3	Vzpostavljeno	6/10	Raven zmogljivosti se lahko na splošno šteje za nadpovprečno.
4	Strokovno	8/10	Raven zmogljivosti se lahko na splošno šteje za zadovoljivo in bi bila za večino organizacij več kot zadostna. Sposobnost se obravnava kot model za druge organizacije.
5	Odlično	9/10	Raven zmogljivosti se lahko šteje za "vodilno v svetu".
6	Popolno	10/10	Ne pričakuje se, da bo katera koli organizacija imela zmogljivosti na tej ravni.

Vir: Gay idr., 2016.

Operacije v kibernetskem prostoru omogočajo uporabo kibernetskih zmogljivosti za doseganje vojaških ciljev v kibernetskem prostoru ali prek njega (NATO, 2018c). Od operacij v drugih domenah se razlikujejo po tem, da se lahko izvajajo tudi v miru (Dalmjin idr., 2020). Zajemajo operacije zagotavljanja delovanja KIS, defenzivne kibernetske operacije, obveščevalne operacije z nadzorom in izvidovanjem kibernetskega prostora ter ofenzivne kibernetske operacije (NATO, 2018c). Prve z ukrepi za vzpostavitev, varovanje in delovanje KIS ohranjajo razpoložljivost, celovitost in zaupnost podatkov ter overitev uporabnika in nepreklicnost (NATO, 2020). Defenzivne operacije z aktivnimi in pasivnimi ukrepi ohranjajo možnost uporabe kibernetskega prostora, obveščevalne zagotavljajo zbiranje podatkov in informacij, ofenzivne pa ustvarjajo učinke v kibernetskem prostoru ali prek njega za dosego vojaških ciljev.

3.1.3 Pregled ugotovitev razvoja kibernetske varnosti NATA

Nato se od začetka 21. stoletja sistematično posveča krepitvi kibernetske obrambe. Od prvega priznanja groženj leta 2006 do vrha v Vilni leta 2023 je razvijal politike, zmogljivosti in sodelovanje z zaveznicami, mednarodnimi organizacijami, industrijo in akademskim svetom ter kibernetsko obrambo uveljavil kot sestavni del kolektivne obrambe. Za logistiko je ta razvoj pomemben, ker odpornost zavezništva temelji tudi na zanesljivem delovanju prometa, transportnih poti in oskrbe, torej na zmogljivostih, ki jih v veliki meri zagotavlja civilni sektor. Kibernetska zaščita pristanišč, železnic, skladišč in informacijskih sistemov za oskrbo zato ni le poslovno vprašanje posameznega podjetja, temveč prispevek k obrambni pripravljenosti države in zavezništva.

3.2 Kibernetska varnost v EU

Kibernetsko varnost EU predstavljamo strnjeno skozi strategijo, zakonodajo s certificiranjem, investicije, razvoj znanj ter druga področja kibernetske politike (povzeto po Plevnik in Ščavničar, 2026). Za logistiko je ureditev EU še posebej pomembna, saj podjetja v oskrbovalnih verigah poslujejo čezmejno in zanje veljajo enotna evropska pravila, promet pa sodi med sektorje, ki jih evropska zakonodaja obravnava prednostno.

3.2.1 Strategija in zakonodaja

Strategija EU za kibernetsko varnost je temeljni dokument za krepitev odpornosti proti kibernetskim grožnjam, ohranjanje odprtega in varnega interneta ter zaščito temeljnih pravic in varnosti v Evropi (Evropska komisija, 2023f). Opredeljuje, kako lahko EU z regulativnimi, naložbenimi in političnimi instrumenti doseže tehnološko suverenost in vodilni položaj v globalnem digitalnem prostoru, ter napoveduje doslej najvišje ravni naložb v digitalni prehod.

Osrednji zakonodajni ukrep je Direktiva o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, ki krepi zaščitne ukrepe v vseh pomembnejših gospodarskih in družbenih sektorjih ter vzpostavlja nacionalne enote za odzivanje na incidente in strateško sodelovanje med članicami (Evropska komisija, 2023a). Med sektorje visoke kritičnosti uvršča tudi promet, poštne in kurirske storitve pa med pomembne subjekte, zato njene obveznosti neposredno zadevajo velik del logističnih podjetij. Pri izvajanju politik ima osrednjo vlogo agencija ENISA (2023a). Akt o kibernetski odpornosti zagotavlja, da se izdelki razvijajo z visokimi standardi kibernetske varnosti že od zasnove (Evropska komisija, 2023b), kar je pomembno tudi za naprave interneta stvari v skladiščih in vozilih.

Akt o kibernetski varnosti uvaja enoten certifikacijski sistem s priznavanjem certifikatov po vsej EU (Evropska komisija, 2023c), kar organizacijam olajša izbiro preverjeno varne opreme in storitev. Akt o kibernetski solidarnosti z evropskim kibernetskim ščitom izboljšuje zaznavanje obsežnih incidentov in vzajemno pomoč med državami članicami (EU, 2023b).

3.2.2 Investicije, znanja in ozaveščenost

EU kibernetsko varnost podpira z obsežnimi naložbami. Raziskave in inovacije financira prek programov Obzorje 2020 in Obzorje Evropa (Evropska komisija, 2023d), Program za digitalno Evropo pa za obdobje 2021 do 2027 načrtuje 1,9 milijarde evrov za zmogljivosti ter široko uvedbo infrastruktur in orodij kibernetske varnosti za javne uprave, podjetja in posameznike (Evropska komisija, 2023g). Kibernetska varnost je vključena tudi v program InvestEU (Evropska komisija, 2023h), razvoj in uvajanje tehnologij pa usklajuje Evropski industrijski, tehnološki in raziskovalni kompetenčni center za kibernetsko varnost (EU, 2023c). Ta sredstva so dosegljiva tudi podjetjem in raziskovalnim skupinam s področja prometa in logistike.

Ker je pomanjkanje usposobljenih kadrov ena največjih ovir, ki jo občutijo tudi logistične organizacije, EU vlaga v znanja in ozaveščenost. Akademija znanj in spretnosti EU za kibernetsko varnost združuje javne in zasebne pobude za odpravo vrzeli v delovni sili (Evropska komisija, 2023k), ozaveščenost pa krepijo pobude, kot je Evropski mesec kibernetske varnosti v sodelovanju z agencijo ENISA (2023b).

3.2.3 Druga področja in pregled ugotovitev

EU se je z načrtom za hitro odzivanje pripravila na obsežne čezmejne kibernetske incidente (Evropska unija, 2023), z ustanovitvijo Skupne kibernetske enote pa je vzpostavila osrednjo platformo za koordinacijo odzivov (Evropska komisija, 2023i). Z orodji za ublažitev tveganj ureja varno uvedbo omrežij 5G (Evropska komisija, 2023j), na katerih bo slonel vse večji del povezane logistike. Med druga področja politike sodijo boj proti kibernetski kriminaliteti v sodelovanju z Europolom, kibernetska diplomacija z možnostjo sankcij proti napadalcem, kibernetska obramba s tesnejšim povezovanjem vojaškega in civilnega sektorja (Evropska komisija, 2023l) ter pomoč tretjim državam pri krepitvi njihovih zmogljivosti (Evropska komisija, 2023e).

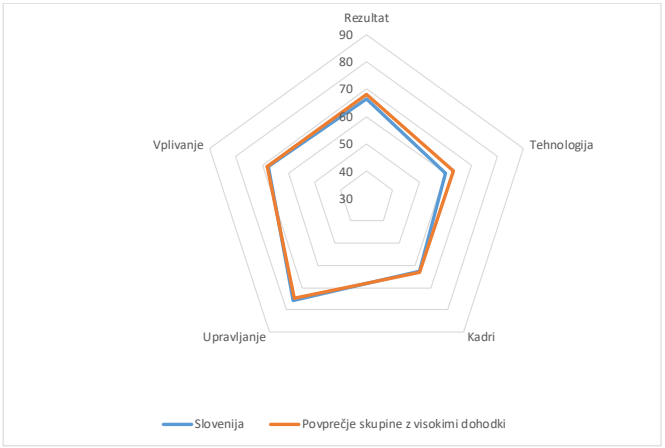
Pregled pokaže, da EU kibernetsko varnost gradi predvsem regulativno in naložbeno, s poudarkom na tehnološki suverenosti, certificiranju, razvoju znanj in mednarodnem sodelovanju. Za logistične organizacije ta ureditev pomeni dvoje. Po eni strani prinaša obveznosti, saj direktiva in nacionalna zakonodaja promet uvrščata med prednostno varovane sektorje, po drugi strani pa priložnosti, od enotnih pravil za čezmejno poslovanje in certificirane opreme do evropskih sredstev za dvig lastne kibernetske odpornosti.

3.3 Študija primera kibernetske varnosti Slovenije

Študija primera obravnava javno objavljene dokumente nacionalnega sistema kibernetske varnosti Slovenije, od strategije in zakonodaje do operativnih organov in programov ozaveščanja (povzeto po Plevnik in Ščavničar, 2026). Posebej izpostavljamo vsebine, pomembne za organizacije, ki so po zakonodaji zavezanci, med njimi tudi podjetja iz sektorja prometa in logistike.

Slovenija se v globalnem indeksu omrežne pripravljenosti uvršča na visoko 27. mesto med 134 državami (glej Sliko 9), pri čemer dosega nadpovprečne rezultate zlasti pri dostopu do tehnologij, predpisih in kakovosti življenja, slabše pa pri vplivu na gospodarstvo (Dutta in Lanvin, 2020). Država ima torej dobro podlago za digitalno poslovanje, ki pa jo mora spremljati ustrezna raven kibernetske varnosti.

	Mesto (od 134)	Rezultat
Indeks omrežne pripravljenosti	**27**	**66,58**
A. Tehnološki steber	**29**	**60,31**
1. podsklop: Dostop	24	83,66
2. podsklop: Vsebina	26	57,10
3. podsklop: Prihodnje tehnologije	35	40,18
B. Steber kadri	**28**	**62,53**
1. podsklop: Posamezniki	34	64,89
2. podsklop: Podjetja	23	65,09
3. podsklop: Vlada	30	57,63
C. Steber upravljanja	**25**	**75,81**
1. podsklop: Zaupanje	28	67,70
2. podsklop: Predpisi	21	83,57
3. podsklop: Vključenost	31	76,16
D. Steber vpliva	**25**	**67,67**
1. podsklop: Gospodarstvo	43	33,47
2. podsklop: Kakovost življenja	9	88,97
3. podsklop: Trajnostni razvoj	18	80,57



Slika 10: Indeks omrežne pripravljenosti – Slovenija.
Vir: Dutta in Lanvin, 2020.

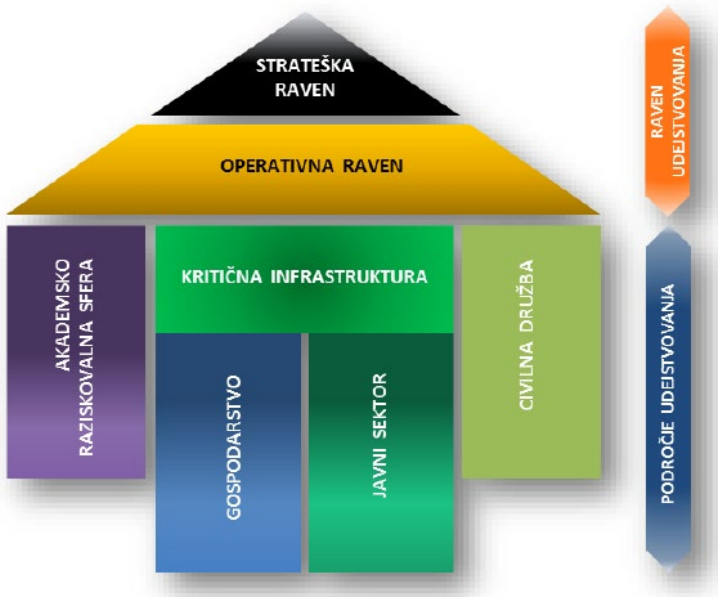
Leta 2016 je bila sprejeta Strategija kibernetske varnosti, ki kibernetsko varnost opredeli kot pomemben integralni dejavnik nacionalne varnosti ter podlago za nemoteno delovanje državnih organov, gospodarstva in življenje posameznikov (Vlada RS, 2016a). Strategija določa osem ciljev, od sistemske ureditve nacionalnega sistema, varnosti državljanov in gospodarstva do zaščite kritične infrastrukture, zatiranja kibernetskega kriminala, razvoja

obrambnih zmogljivosti, delovanja sistemov ob velikih nesrečah in mednarodnega sodelovanja, za vsak cilj pa opredeli ukrepe (glej Tabelo 5). Sistem organizira na treh ravneh, strateški, operativni in ravni konkretnih ukrepov (glej Sliko 10). Za gospodarstvo, vključno z logističnimi podjetji, sta pomembna zlasti cilja kibernetske varnosti v gospodarstvu in zaščite kritične infrastrukture.

Tabela 53: Pregled ciljev strategije kibernetske varnosti in ukrepov.

Cilj	Ukrep
Okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti.	- vzpostavitev osrednje koordinacije nacionalnega sistema zagotavljanja kibernetske varnosti; - kadrovska in tehnološka okrepitev organov na operativni ravni sistema zagotavljanja kibernetske varnosti skupaj z vzpostavitvijo SIGOV-CERT; - redna udeležba na mednarodnih vajah s področja kibernetske varnosti ter izvedba nacionalnih vaj; - postopna nadgradnja omrežja državnih organov HKOM z opremo, ki je ustrezno potrjena s strani slovenskih organov kot varna in primerna za uporabo; - vzpostavitev kompetentnega preverjanja varnosti in funkcionalnosti informacijske opreme v okviru obstoječih in novo vzpostavljenih organov.
Varnost državljanov v kibernetskem prostoru.	- redno izvajanje programov ozaveščanja na področju kibernetske varnosti; - uvedba vsebin s področja kibernetske varnosti v sistem izobraževanja in usposabljanja.
Kibernetska varnost v gospodarstvu.	- spodbujanje razvoja in vpeljave novih tehnologij na področju kibernetske varnosti; - redno izvajanje programov ozaveščanja na področju kibernetske varnosti za gospodarske subjekte.
Zagotavljanje delovanja kritične infrastrukture v sektorju informacijsko-komunikacijske podpore.	redno ocenjevanje tveganj za delovanje kritične infrastrukture sektorja informacijsko-komunikacijske podpore, načrtovanje ustreznih ukrepov za zaščito ter posodabljanje ocene tveganj na tem področju
Zagotavljanje kibernetske varnosti na področju javne varnosti in zatiranje kibernetskega kriminala.	- implementacija ustreznih kibernetskih zmogljivosti za varovanje informacijskih in komunikacijskih sistemov policije; - redno usposabljanje s področja kibernetske varnosti za organe pregona, ki sodelujejo pri razvoju kibernetskih zmogljivosti za področje javne varnosti in pri zatiranju kibernetskega kriminala; - redno posodabljanje zakonodaje in postopkov skladno z razvojem informacijsko-komunikacijskih tehnologij.
Razvoj obrambnih kibernetskih zmogljivosti.	razvoj ustreznih kibernetskih zmogljivosti za varovanje obrambnih komunikacijskih in informacijskih sistemov
Zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah.	zagotovitev pogojev za nemoteno delovanje ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah
Krepitev nacionalne kibernetske varnosti z mednarodnim sodelovanjem.	zagotovitev pogojev za sodelovanje slovenskih strokovnjakov v relevantnih mednarodnih delovnih telesih in združenjih s področja kibernetske varnosti

Vir: Vlada RS, 2016a.

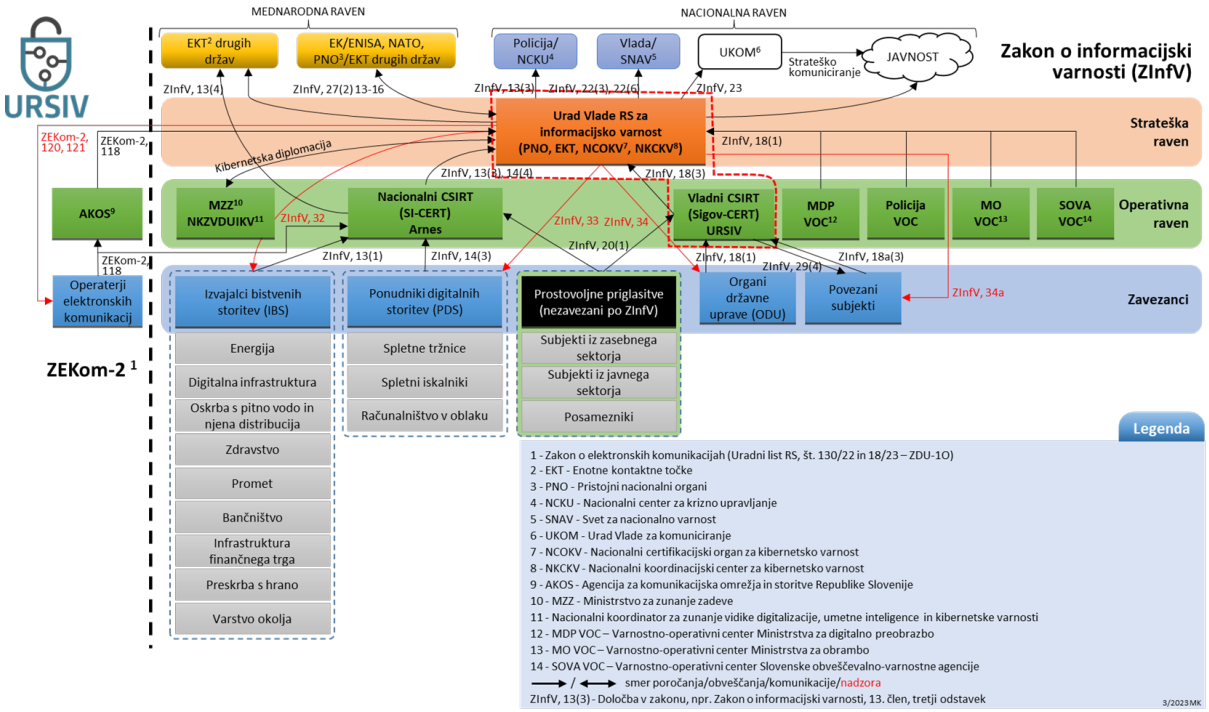


Slika 11: Prikaz sistema zagotavljanja kibernetske varnosti RS.
Vir: Vlada RS, 2016a.

Za začetno operacionalizacijo sistema je vlada leta 2017 naloge na strateški ravni zaupala Uradu Vlade Republike Slovenije za varovanje tajnih podatkov (Sklep o dopolnitvi Sklepa o ustanovitvi, nalogah in organizaciji UVTP, 2017). Leta 2021 jih je prevzel Urad Vlade Republike Slovenije za informacijsko varnost (v nadaljevanju URSIV), ki kot samostojna vladna služba opravlja naloge pristojnega nacionalnega organa po zakonodaji s področja informacijske varnosti (Odlok o ustanovitvi, nalogah in organizaciji URSIV, 2021; URSIV, 2023a).

Pomemben premik k celoviti zasnovi sistema je prinesel Zakon o informacijski varnosti iz leta 2018, s katerim je bila v slovenski pravni red prenesena evropska direktiva o varnosti omrežij in informacijskih sistemov (ZInfV, 2018). Zakon je opredelil zavezance, med njimi izvajalce bistvenih storitev s področij energije, digitalne infrastrukture, oskrbe s pitno vodo, zdravstva, prometa, bančništva, infrastrukture finančnega trga, preskrbe s hrano in varstva okolja, ponudnike digitalnih storitev ter organe državne uprave. Promet je torej že od začetka med prednostno varovanimi sektorji, zato so med zavezanci tudi večja logistična podjetja. Zavezanci morajo opredeliti svoje najpomembnejše informacijske sisteme, izvajati analizo in oceno tveganj, vzdrževati dokumentiran sistem upravljanja varovanja informacij in neprekinjenega poslovanja z načrtom obnovitve ter načrtom odzivanja na incidente in incidente priglašati. Nacionalno strukturo so poleg URSIV sestavljali še odzivni centri in drugi pristojni organi (glej Sliko 11) (Kavčič, 2023). Zahteve zakona se vsebinsko ujemajo s tem, kar oskrbovalna veriga od partnerjev tako ali tako pričakuje, torej zanesljivo in neprekinjeno delovanje.

Junija 2025 je stari zakon nadomestil Zakon o informacijski varnosti ZInfV-1, ki v slovenski pravni red prenaša direktivo NIS 2 (ZInfV-1, 2025). Krog zavezancev se je bistveno razširil in po novem zajema bistvene in pomembne subjekte, pri čemer med prve sodi tudi promet, poštne in kurirske storitve pa med pomembne subjekte (Evropska komisija, 2023a). Zavezanci se morajo sami priglasiti v evidenco ter izvajati ukrepe za obvladovanje tveganj, od varnostnih politik in osnovne kibernetske higiene do usposabljanja, za izvajanje pa je izrecno odgovorno tudi vodstvo subjekta. Pomembne incidente je treba priglasiti pristojni skupini CSIRT z zgodnjim sporočilom nemudoma oziroma najpozneje v 24 urah po zaznavi, s priglasitvijo in začetno oceno resnosti najpozneje v 72 urah ter s končnim poročilom najpozneje v enem mesecu (ZInfV-1, 2025). Za velik del logističnih podjetij, ki dosegajo velikostna merila, kibernetska varnost s tem ni več le dobra praksa, temveč zakonska obveznost in pogoj za sodelovanje v oskrbovalnih verigah.



Slika 12: Shema nacionalnega sistema zagotavljanja informacijske varnosti.
Vir: Kavčič, 2023.

ZInfV-1 ureja tudi kibernetsko obrambo, ki jo 38. člen opredeljuje kot celoto ukrepov in dejavnosti za preprečevanje kibernetskih groženj in incidentov ter ublažitev njihovih vplivov na vseh treh plasteh kibernetskega prostora (ZInfV-1, 2025). Njeno izvajanje na ravni državnih organov po 39. členu usklajujejo in izvajajo pristojni nacionalni organ, skupine CSIRT, ministrstva, pristojna za obrambo, za upravljanje informacijskih in komunikacijskih sistemov ter za zunanje in notranje zadeve, Policija, Slovenska

obveščevalno-varnostna agencija in drugi državni organi v skladu s svojimi pristojnostmi. Koordinacijo izvaja pristojni nacionalni organ s koordinacijsko skupino, za zgodnje zaznavanje groženj pa vzpostavi situacijski center kibernetske obrambe (prav tam).

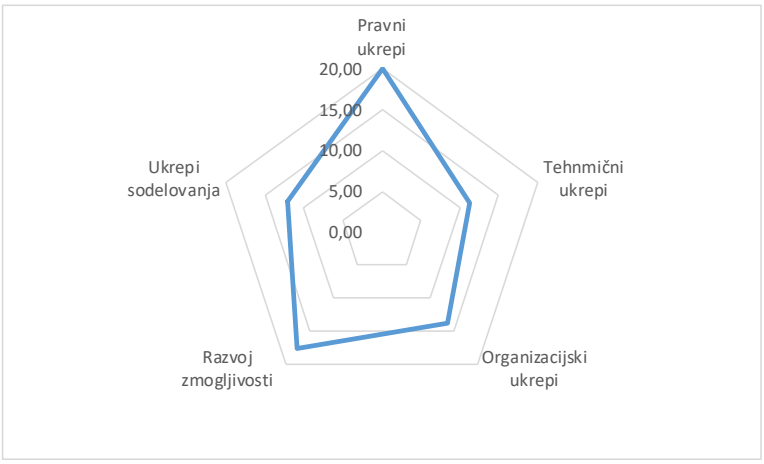
Zakon dopolnjujejo podzakonski akti, med njimi Uredba o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev (Uredba o določitvi bistvenih storitev, 2019) ter uredbe o varnostni dokumentaciji in varnostnih ukrepih. Leta 2021 je bil kot vodilo za zavezance izdelan Nacionalni načrt odzivanja na kibernetske incidente (v nadaljevanju NOKI), ki določa, komu, kdaj in kako priglasiti kibernetske incidente, njihovo upravljanje poenoti z enotno taksonomijo in metodologijo poročanja ter ureja usklajen odziv na državni ravni (Vlada RS, 2021). Zavezanci morajo pripraviti interne načrte odzivanja in poročati o incidentih nad določenim pragom, priporočljivo pa je tudi prostovoljno poročanje o manjših incidentih. Prav NOKI je podlaga za klasifikacijo incidentov, ki jo uporabljamo v vajah na koncu poglavja.

Osrednji operativni organ za gospodarstvo in javnost je nacionalni odzivni center SI-CERT, ustanovljen leta 1995 v okviru javnega zavoda Arnes (ARNES, 2023e). Rešuje kibernetske incidente, svetuje ob vdorih in okužbah ter izdaja opozorila in letna poročila. Število obravnavanih incidentov iz leta v leto raste, s 3177 leta 2021 na 4123 leta 2022, 4280 leta 2023 in 4587 leta 2024, med njimi pa prevladujejo ribarjenje in spletne goljufije (ARNES, 2025). Prijava incidentov je za zavezance obvezna, vsi drugi poslovni subjekti in posamezniki, torej tudi logistična podjetja, ki niso zavezanci, pa lahko incident prijavijo prostovoljno in dobijo pomoč pri identifikaciji, zamejitvi in odpravi posledic (ARNES, 2023b). SI-CERT s programom Varni na internetu ozavešča javnost s posebnim poudarkom na malih podjetjih in samostojnih podjetnikih (ARNES, 2023c), kar je dragoceno tudi za manjše prevoznike in špediterje. Za incidente v informacijskih sistemih državne uprave je pristojen SIGOV-CERT, ki deluje v okviru URSIV (URSIV, 2023e), inšpekcijski nadzor nad zavezanci pa izvajajo inšpektorji URSIV (ZInfV, 2018).

URSIV poleg koordinacije sistema objavlja povabila na evropske razpise za sofinanciranje kibernetske varnosti, vzpostavlja mrežo šol za kibernetsko varnost ter organizira usposabljanja, tekmovanja in sodelovanje na mednarodnih vajah (URSIV, 2023b, 2023c, 2023d). Do konca leta 2023 je dvakrat razglasil stanje povečane ogroženosti, in sicer ob kritični ranljivosti v javanski knjižnici Apache Log4j (URSIV, 2021a) in ob ranljivosti strežnikov Microsoft Exchange (URSIV, 2021b). Oba primera kažeta, kako lahko ranljivost v razširjeni programski opremi čez noč ogrozi tudi poslovne sisteme logističnih podjetij.

Resolucija o strategiji nacionalne varnosti opozarja, da ranljivost sodobne družbe izhaja iz odvisnosti od neprekinjenega in zanesljivega delovanja informacijskih tehnologij, zaradi česar je lahko ogroženo izvajanje temeljnih funkcij države in družbe (ReSNV-2, 2019). Ocena kibernetskih tveganj iz leta 2018 je klasificirala grožnje, akterje in vektorje napada ter opozorila, da lahko Slovenija postane tarča vplivanja na demokratične procese in napadov na kritično infrastrukturo (Kavčič, 2018). Kazenskopravni okvir zagotavlja Kazenski zakonik, ki v 221. členu opredeljuje kazniva dejanja napadov na informacijske sisteme, od vdorov in spreminjanja podatkov do oviranja delovanja sistemov, s posebnim poudarkom na kritični infrastrukturi (Kazenski zakonik [KZ-1], 2023).

Za varno elektronsko poslovanje z državnimi organi in med podjetji je vzpostavljen sistem kvalificiranih digitalnih potrdil (Ministrstvo za digitalno preobrazbo, 2023), ki so vsakdanje orodje tudi v logistiki, od oddaje carinskih dokumentov do podpisovanja pogodb. Da sistem ni brez pomanjkljivosti, je pokazala revizija Računskega sodišča (2021), ki je za obdobje od 2016 do 2019 ugotovila neučinkovitost vlade in pristojnih organov, od zamud pri sprejemanju predpisov do kadrovske in finančne podhranjenosti ter pomanjkljivega ozaveščanja. Mednarodne primerjave Slovenijo kljub temu uvrščajo razmeroma visoko, indeks kibernetske varnosti ITU jo je globalno postavil na 67. mesto (glej Sliko 12) (ITU, 2021). Mejnike razvoja prikazuje Slika 13.



Skupna ocena	Pravni ukrepi	Tehnmični ukrepi	Organizacijski ukrepi	Razvoj zmogljivosti	Ukrepi sodelovanja
74,93	20,00	11,38	13,71	17,72	12,11

Slika 13: Global Cybersecurity Index 2020 – Slovenija.
Vir: ITU, 2021.



Slika 14: Mejniki razvoja kibernetske varnosti Slovenije.
Vir: lasten.

Univerzitetna založba
Univerze v Mariboru

4 Vaje

Vaje in rešitve so prirejene po zbirki praktičnih vaj iz učbenika Kibernetski prostor in Slovenska vojska (Plevnik in Ščavničar, 2026). Razvrščanje incidentov sledi taksonomiji NOKI (Vlada RS, 2021) in stopnjam po ZInfV (2018).

Vaja 1: Klasifikacija kibernetskega incidenta – določitev vrste incidenta

Namen in cilj

Udeleženci se naučijo:

- prepoznati osnovne vrste kibernetskih incidentov,
- uporabiti klasifikacijo po vrsti in vplivu,
- utemeljiti svojo odločitev z opisom simptomov in posledic.

Predpogoji

- poznavanje osnov informacijskih sistemov (računalnik, omrežje, aplikacija),
- dostop do primera opisa incidenta (spodaj).
  Ni potrebna tehnična oprema — vaja je lahko tudi "*table-top*" ali pisna vaja.

Navodilo za izvedbo

1. Preberi spodaj naveden **primer incidenta**.
2. Ugotovi, **katera vrsta incidenta** je najverjetnejša.
3. Določi tudi **glavni učinek incidenta** (zaupnost, celovitost, razpoložljivost).

4. Utemelji svojo odločitev v 3–5 stavkih.

Primer scenarija

Opis dogodka:

V torek ob 10:15 je sistem za upravljanje skladišča (*WMS*) nenadoma postal počasnejši. Uporabniki so poročali, da aplikacija pogosto zamrzne in da se na strežniku pojavljajo neznane datoteke z naključnimi imeni (npr. tmp1241.exe).

Analiza je pokazala, da se v ozadju izvaja proces, ki obremenjuje procesor in omrežje ter komunicira z zunanjim IP-naslovom v tujini. Protivirusni program je prijavil "*Trojan.Generic*".

Po zaustavitvi procesa se je delovanje normaliziralo, vendar so se logi naknadno izbrisali.

Naloga

A) Katera vrsta incidenta je to? (obkroži ali zapiši številko)

1. Žaljiva / zlonamerna vsebina
2. Zlonamerna koda
3. Zbiranje informacij
4. Poskus vdora
5. Vdor
6. Razpoložljivost
7. Varnost informacijskih virov
8. Goljufije
9. Ranljivost
10. Drugo

B) Kateri vidik varnosti je bil prizadet?

- ☐ Zaupnost (*Confidentiality*)
- ☐ Celovitost (*Integrity*)
- ☐ Razpoložljivost (*Availability*)

C) Utemelji svojo odločitev:
(zapiši 3–5 stavkov)

Vaja 2: Klasifikacija kibernetskega incidenta – "phishing" in kraja poverilnic

Namen in cilj

Udeleženci:

- spoznajo značilnosti socialnega in komunikacijskega napada,
- razvrstijo incident v ustrezno kategorijo,
- ocenijo prizadeti varnostni cilj (zaupnost, celovitost, razpoložljivost),
- predlagajo osnovne ukrepe.

Predpogoji

Ni potrebna posebna tehnična oprema.

Zadošča poznavanje e-pošte in osnovnih konceptov zaupnosti podatkov.

Navodilo za izvedbo

1. Preberi primer spodaj.
2. Določi **vrsto incidenta** po taksonomiji.
3. Označi **prizadeti varnostni cilj**.

4. Napiši **kratko utemeljitev** in **predlagaj 2 ukrepa** za preprečitev podobnih primerov.

Primer scenarija

Opis dogodka:

Računovodkinja logističnega podjetja prejme e-pošto, ki je videti kot sporočilo banke z naslovom "Nujno potrdilo plačila za dobavitelja".

V sporočilu je povezava do spletne strani, ki je videti kot spletna banka. Zaposlena se prijavi z uporabniškim imenom in geslom. Stran po prijavi javi "napako", a v ozadju podatke pošlje napadalcu.

Naslednji dan so na računu podjetja zaznane nepooblaščene transakcije.

Naloga

A) Katera vrsta incidenta je to?

1. Žaljiva / zlonamerna vsebina
2. Zlonamerna koda
3. Zbiranje informacij
4. Poskus vdora
5. Vdor
6. Razpoložljivost
7. Varnost informacijskih virov
8. Goljufije
9. Ranljivost
10. Drugo

B) Kateri varnostni cilj je prizadet?

- ☐ Zaupnost
- ☐ Celovitost
- ☐ Razpoložljivost

C) Utemelji svojo odločitev (3–5 stavkov):
(navedi ključne indice, npr. zavajanje, kraja poverilnic, finančna škoda)

D) Predlagaj dva ukrepa, s katerima bi lahko preprečili tak incident.

Vaja 3: Klasifikacija kibernetskega incidenta glede na resnost (lažji, težji, kritični)

Namen in cilj

Udeleženci se naučijo:

- razlikovati med lažjimi, težjimi in kritičnimi incidenti,
- oceniti vpliv incidenta na poslovanje in čas odziva,
- povezati resnost incidenta z ustreznimi ukrepi in postopkom poročanja.

Predpogoji

- poznavanje osnovnih vrst incidentov (iz prejšnjih vaj),
- razumevanje pojmov: vpliv (*impact*), obseg (*scope*), čas trajanja, prizadeti sistemi.

Navodilo za izvedbo

1. Preberi tri opise dogodkov spodaj.
2. Za vsak primer določi, ali gre za **lažji**, **težji** ali **kritični** incident.
3. Utemelji odločitev z 2–3 stavki.
4. (Izbirno) Predlagaj ustrezen ukrep in čas za odziv.

Primeri scenarijev

– Primer A

V enem od skladišč uporabnik pomotoma odpre e-poštno priponko, ki vsebuje makro v Excel datoteki. Protivirusni program okužbo zazna in datoteko samodejno izbriše. Sistem deluje naprej brez motenj, poročilo je zabeleženo v logu.

– Primer B

V sistemu za sledenje pošiljk pride do vdora v uporabniški račun. Napadalec pridobi dostop do seznamov strank in delno spremeni podatke o naslovih dostave. Odkrili so ga po dveh urah, sistem je bil za kratek čas onemogočen, izgubljenih je bilo nekaj naročil.

– Primer C

Centralni ERP strežnik, ki povezuje več distribucijskih centrov, preneha delovati zaradi šifrirne zlonamerne kode (*ransomware*). Vsi procesi so zaustavljeni, podatki so šifrirani, *backupi* nedostopni. Ocena škode presega več sto tisoč evrov, poslovanje stoji več kot 24 ur.

Naloga

Primer	Vrsta incidenta po resnosti	Utemeljitev	Predlagani ukrep in čas odziva
A	☐ Lažji ☐ Težji ☐ Kritični		
B	☐ Lažji ☐ Težji ☐ Kritični		
C	☐ Lažji ☐ Težji ☐ Kritični		

Vaja 4: Razvrstitev kibernetskih incidentov na podlagi žrtev in učinka

Namen in cilj

Udeleženci:

- razumejo, da imajo kibernetski incidenti različne **ciljne žrtve** (posamezniki, organizacije, partnerji, javnost),
- znajo določiti **učinek incidenta** (npr. kraja podatkov, prekinitev storitve, finančna izguba, izguba zaupanja),
- razvrstijo primere v ustrezne kategorije in utemeljijo svojo odločitev.

Predpogoji

- osnovno razumevanje vrst in resnosti incidentov (prejšnje vaje),
- ni potrebna tehnična oprema — vaja je pisna ali skupinska (*table-top*).

Navodilo za izvedbo

1. Preberi tri primere spodaj.
2. Za vsak primer določi:
   - **Kdo je žrtev incidenta** (posameznik, organizacija, dobavitelj, stranka, javnost ipd.),
   - **Kakšen je glavni učinek** (kraja podatkov, motnja poslovanja, finančna škoda, ugled ipd.).
3. Utemelji svojo odločitev v 2–3 stavkih.

Primeri scenarijev

– Primer A

Skladiščni delavec prejme e-pošto, ki vsebuje lažno prijavo v kadrovski sistem. Po vnosu gesla dobi napadalec dostop do osebnih podatkov zaposlenih (ime, naslov, EMŠO).

– Primer B

Napadalec vdre v informacijski sistem dobavitelja in za 12 ur ohromi dobavo surovin. Glavno podjetje ne more dokončati naročil in zamudi rok dostave.

– Primer C

Stranke logističnega podjetja ugotovijo, da je bil javno objavljen seznam z njihovimi osebnimi podatki in številkami naročil. Dogodek se razširi po medijih, podjetje prejme pritožbe in izgubi nekaj poslovnih partnerjev.

Naloga

Primer	Žrtev incidenta	Učinek	Utemeljitev
A			
B			
C			

Vaja 5: Ocena stopnje kibernetskega incidenta na podlagi kazalnikov učinka in vpliva

Namen in cilj

Udeleženci:

- spoznajo, da se resnost incidenta ne določa le po vrsti, ampak tudi po **učinku** (kaj se zgodi) in **vplivu** (koga in koliko prizadene),
- uporabijo dve skupini kazalnikov za določitev **končne stopnje incidenta**,
- ugotovijo, ali je incident **pod pragom ali nad pragom obveznega poročanja** (npr. po NOKI ali internih postopkih),
- predlagajo ustrezne postopke ukrepanja.

Predpogoji

- poznavanje osnov vrst incidentov in pojmov CIA (*Confidentiality*, *Integrity*, *Availability*),
- dostop do primera scenarija (v nadaljevanju),
- tabela kazalnikov učinka in vpliva (poenostavljena iz uradnega modela).

Navodilo za izvedbo

1. Preberi spodnji **primer incidenta**.
2. Izpolni tabelo **kazalnikov učinka** in **kazalnikov vpliva**.

3. Na podlagi kombinacije določi **končno stopnjo incidenta**.
4. Odloči, ali je incident **pod pragom** ali **nad pragom obveznega poročanja**.
5. Utemelji svojo odločitev v nekaj stavkih.

Primer scenarija

Opis dogodka:

Podjetje za logistično distribucijo uporablja centralni sistem za naročanje in sledenje pošiljk (ERP/WMS).

Zaradi ranljivosti v vtičniku (*plug-inu*) spletnega vmesnika napadalec pridobi dostop do strežnika in kopira bazo s podatki o 12.000 strankah (ime, e-naslov, naslovi, številke naročil).

Incident traja približno 5 ur, nato varnostna ekipa izolira sistem. Storitev sledenja je bila 2 uri nedosegljiva. Podatki so bili verjetno kopirani, vendar ne poškodovani.

Dogodek se razširi v medijih, nekaj strank vloži pritožbe zaradi razkritja podatkov.

Kazalniki učinka (A)

Parameter učinka	Opis dogodka	Stopnja ogroženosti
Razpoložljivost		
Zaupnost		
Celovitost		
Moteno delovanje		
Finančna škoda		
SKUPNA ocena učinka		

Kazalniki vpliva (B)

Parameter vpliva	Opis dogodka	Stopnja vpliva
Število prizadetih uporabnikov		
Prekinitev storitve		
Posledice za funkcije		
Medresorski učinki / ugled		
Varnost države / državljanov		
SKUPNA ocena vpliva		

Določitev končne stopnje incidenta

Kombinacija učinka in vpliva	Končna stopnja incidenta	Prag poročanja
Učinek: ZELO VISOKA / VISOKA + Vpliv: VISOKA	Težji incident – nad pragom	Obvezno poročanje (npr. C3 ali višje)

Utemeljitev

Vaja 6: Določitev stopnje kibernetskega incidenta po ZInfV in obveščanje pristojnih organov

Namen in cilj

Udeleženci:

- razumejo sistem stopnjevanja kibernetskih incidentov po **ZInfV (C1–C6)**,
- znajo na podlagi opisa incidenta določiti njegovo **stopnjo (C-nivo)**,
- vedo, **kateri odzivni center (SI-CERT, SIGOV-CERT, PNO, državni SOC)** mora biti obveščen,
- razumejo logiko postopkov obveščanja in posvetovanja med deležniki.

Predpogoji

- poznavanje osnov kibernetskih incidentov,
- dostop do tabele klasifikacije (Preglednica 3 po ZInfV),
- vaja poteka brez tehničnih orodij (pisno ali skupinsko).

Navodilo za izvedbo

1. Preberi **tri opise incidentov** spodaj.
2. Na podlagi opisa oceni, kateri **C-nivo (C1–C6)** najbolj ustreza.
3. Vpiši, **kdo mora biti obveščen** (zavezanec, SI-CERT, SIGOV-CERT, PNO).
4. Utemelji svojo odločitev v 2–3 stavkih.

Preglednica stopnjevanja po ZInfV

Tabela 54

Stopnja	Opis	Primer
C1 – Kritični incident	Povzroči resno motnjo delovanja države, obrambe, notranje varnosti ali sistema zaščite in reševanja.	Napad na nacionalno omrežje ali krizni center.
C2 – Zelo pomemben incident	Močan negativni vpliv na kritično infrastrukturo ali občutljive podatke.	Napad na energetski sistem, policijo ali več ministrstev.
C3 – Pomemben incident	Vpliva na izvajalce bistvenih storitev ali dobavno verigo kritične infrastrukture.	Napad na logistično podjetje, ki oskrbuje bolnišnice.
C4 – Srednji incident	Vpliv na gospodarstvo ali del državne uprave, manjša motnja storitev.	Izpad spletnega portala državne agencije za nekaj ur.
C5 – Lažji incident	Manjši vpliv ali priprava na napad; zaznane nenavadne aktivnosti.	Poskus *phishinga* ali skeniranje portov.
C6 – Varnostni dogodek	Brez dejanskega vpliva na storitve; informativen dogodek.	Odkrivanje sumljivega e-poštnega prometa brez posledic.

Primeri za razvrščanje

– Primer A

Na spletni strani državnega organa je vgrajena zlonamerna koda, ki preusmerja obiskovalce na lažno spletno mesto. Napad traja več ur, prizadetih je več tisoč uporabnikov, med njimi tudi državni uslužbenci.

Sistem se obnovi po 6 urah, a incident se razširi v medijih.

– Primer B

Logistično podjetje, ki dobavlja medicinske pripomočke bolnišnicam, doživi izpad *WMS* in *ERP* sistemov zaradi *ransomware* napada. Distribucija je za 24 ur ustavljena, več bolnišnic poroča o pomanjkanju zalog.

– Primer C

Analitik v podjetju zazna poskus prijave v *SIEM* iz tujega IP naslova. Prijava ni uspela, sistem ni bil ogrožen, napad je bil zabeležen v *logih*.

Naloga

Primer	Ocenjena stopnja (C1–C6)	Kdo mora biti obveščen?	Utemeljitev
A			
B			
C			

Logika poročanja in obveščanja

Tabela 55

Vloga	Naloga / Odgovornost	Kdaj ukrepa?
Zavezanec	Zazna incident, oceni stopnjo, poroča brez odlašanja SI-CERT ali SIGOV-CERT	C1–C5
SI-CERT / SIGOV-CERT	Potrdi ali uskladi stopnjo, obvesti PNO	pri vseh potrjenih incidentih
PNO (Posebna nacionalna organizacija)	Določi končno stopnjo, koordinira med odzivnimi centri	C1–C3 (kritični, pomembni, zelo pomembni)
Državni SOC (MO, Policija, SOVA)	Poroča neposredno PNO, kadar gre za pomemben vpliv	po ZInfV, kadar gre za C1–C2



Vaja 7: Poročanje in stopnjevanje kibernetskih incidentov v skladu z ZInfV

Namen in cilj

Udeleženci:

- razumejo obveznost priglasitve incidentov po **ZInfV**,
- znajo prepoznati, **kdaj** in **komu** je treba incident prijaviti,
- razvrstijo incident v ustrezno **stopnjo (C1–C6)**,
- poznajo vloge deležnikov (zavezanec, SI-CERT, SIGOV-CERT, PNO, SOC).

Predpogoji

- poznavanje osnov razvrščanja po učinku in vplivu (prejšnja vaja),
- preglednica s **stopnjami incidentov C1–C6** (glej spodaj).

Navodilo za izvedbo

1. Določi, **kateri deležnik** mora incident **priglasiti** in **komu**.
2. Razvrsti incident v ustrezno **stopnjo (C1–C6)**.
3. Utemelji svojo odločitev (2–3 stavke).
4. Določi, ali je potrebno **obvestiti PNO**.

Povzetek postopka po ZInfV

Tabela 56

Deležnik	Naloga / vloga
Zavezanec (podjetje, izvajalec storitev, organ)	brez odlašanja priglasi incident SI-CERT ali SIGOV-CERT
SI-CERT / SIGOV-CERT	določi predhodno stopnjo incidenta (C1–C6) in obvesti PNO
PNO (pristojni nacionalni organ)	potrdi ali spremeni stopnjo incidenta; usklajuje odziv
Državni organi z lastnimi SOC (npr. MO, Policija, SOVA)	sami obvestijo PNO o incidentih z "pomembnim vplivom"
Usklajevanje	odzivni centri in PNO se lahko posvetujejo in uskladijo oceno

Preglednica stopenj incidentov (poenostavljen izvleček iz ZInfV)

Tabela 57

Stopnja	Naziv	Kratek opis
C1	Kritični incident	Motnje delovanja države, obrambnih ali varnostnih sistemov.
C2	Zelo pomemben incident	Napad na kritično infrastrukturo ali občutljive podatke države.
C3	Pomemben incident	Vpliv na izvajalce bistvenih storitev ali dobavno verigo kritične infrastrukture.
C4	Srednji incident	Manjši vpliv na omrežja, gospodarske dejavnosti ali dobavne verige.
C5	Lažji incident	Posamezni vpliv ali priprava na napad (npr. poskus vdora).
C6	Varnostni dogodek / grožnja	Brez vpliva na sisteme, zgolj zaznane aktivnosti ali grožnja.

Scenarij

Opis dogodka:

Logistično podjetje, ki oskrbuje več državnih ustanov, zazna več nepooblaščenih poskusov prijave v svoj portal za elektronsko naročanje (več kot 5000 poskusov v eni uri).

Napad izvira iz tujine in uporablja avtomatizirane skripte ("*credential stuffing*"). Do vdora v sistem ni prišlo, vendar so bile zaznane poskusi tudi na partnerskih strežnikih enega izvajalca bistvenih storitev.

Incident je bil prijavljen notranjemu IT-oddelku. Sistem deluje normalno, vendar obstaja možnost, da gre za pripravo večjega napada.

Naloga

Postavka	Odgovor
Zavezanec / prijavitelj	
Koga mora obvestiti	
Predlagana stopnja incidenta	
Utemeljitev	
Obvestilo PNO (da/ne)	

Vaja 8: Določitev praga in časovnega okvira poročanja kibernetskega incidenta

Namen in cilj

Udeleženci:

- razumejo, kdaj je poročanje o incidentu **obvezno** in kdaj **prostovoljno**,
- znajo uporabiti **časovne okvire poročanja** (začetno, vmesno, končno),
- povežejo **stopnjo incidenta (C1–C6)** s **postopki in roki poročanja**,
- vadijo pripravo **prvega poročila** in določitev nadaljnjih korakov.

Predpogoji

- Poznavanje klasifikacije incidentov (C1–C6) iz prejšnje vaje.
- Dostop do preglednic 4, 5 in 6 iz ZInfV (vaja jih povzema spodaj).

Navodilo za izvedbo

1. Določi **stopnjo incidenta (C1–C6)** glede na opis.
2. Označi, ali gre za **obvezno** ali **prostovoljno poročanje**.
3. V tabelo vpiši časovne roke za začetno, vmesno in končno poročilo.
4. Na kratko utemelji svojo odločitev.

Povzetek iz ZInfV

– Prag poročanja

Tabela 58

Stopnja	Poročanje	Opomba
C1–C5	Obvezno poročanje	Takoj, brez odlašanja.
C6 (verjetnost prehoda)	Priporočeno poročanje	Če obstaja možnost stopnjevanja.
C6 (brez vpliva)	Prostovoljno tedensko poročanje	Informativno – pomaga pri analizi groženj.

– Časovni okvir poročanja (zavezanci → SI-CERT / SIGOV-CERT)

Tabela 59

Stopnja	Začetno poročanje	Vmesno poročanje	Končno poročanje
C1	Nemudoma	Vsakih 6 ur	10 dni
C2	V 12 urah	Po potrebi / 5 dni	5 dni
C3	V 24 urah	72 ur	Po zaključku
C4	Po potrebi	48 ur	Po zaključku
C5	Po potrebi	48 ur	Po zaključku
C6	/	/	1× tedensko (prostovoljno)

– Časovni okvir poročanja (odzivni centri → URSIV)

Tabela 60

Stopnja	Začetno	Vmesno	Končno
C1	Nemudoma	Po potrebi	10 dni
C2	Nemudoma	Po potrebi	5 dni
C3	Nemudoma	Po potrebi	72 ur
C4	V 24 urah	/	1× tedensko
C5	/	/	1× tedensko
C6	/	/	1× tedensko

Scenarij

Opis dogodka:

Podjetje za logistične storitve zazna nenavaden promet na svojem poštnem strežniku. Analiza pokaže, da gre za napad z zlonamerno kodo, ki se širi preko priponk v elektronski pošti.

Približno 40 zaposlenih je odprlo priponke, 5 računalnikov je okuženih in izoliranih. Napad se ni razširil na strežnike, vendar je del poslovne e-pošte za 3 ure nedosegljiv. Incident je zabeležen, forenzična ekipa že dela na odpravi, podjetje je zavezanec po ZInfV (kritična logistična storitev).

Naloga

Postavka	Odgovor
Stopnja incidenta	
Obveznost poročanja	
Začetno poročilo (od zaznave)	
Vmesno poročilo (časovni okvir)	
Končno poročilo (časovni okvir)	
Utemeljitev	

Vaja 9: Prvo poročilo o kibernetskem incidentu

Namen in cilj

Udeleženci:

- razumejo pomen **pravočasne in popolne prijave** incidenta odzivnemu centru (SI-CERT ali SIGOV-CERT),
- znajo **pripraviti prvo poročilo** v 24 urah od zaznave incidenta,
- razumejo, **katere informacije** so bistvene za razvrstitev in nadaljnje ukrepanje,
- spoznajo osnovna pravila **komunikacije in varovanja podatkov** med zavezancem, odzivnim centrom in PNO.

Predpogoji

- predhodno znanje o klasifikaciji (C1–C6) in kazalnikih učinka/vpliva,
- osnovno razumevanje postopka zaznave in priglasitve (ZInfV, poglavje 4.1).

Navodilo za izvedbo

Izpolni spodnji **obrazec prvega poročila** glede na zgornji scenarij. (Polja, označena z *priporočeno vsebino,* lahko udeleženec dopolni po lastni presoji.)

Scenarij

Opis dogodka:

Družba *TransLog d.o.o.*, izvajalec bistvene logistične storitve za državne rezerve, zazna nepooblaščen dostop do svojega strežnika za e-naročanje.

Dogodek je bil zaznan v petek ob 08:40, ko so uporabniki poročali o počasnem delovanju sistema.

Administrator je v dnevnikih zaznal več neuspešnih prijav in eno uspešno prijavo z zunanjega IP naslova iz tujine.

Do sprememb podatkov ni prišlo, a obstaja možnost kraje poslovnih dokumentov. Sistem je bil začasno odklopljen, gesla spremenjena, odzivni center je bil obveščen po telefonu ob 09:15.

Zavezanec mora v 24 urah poslati prvo pisno poročilo po ZInfV.

Naloga

PRVO POROČILO O KIBERNETSKEM INCIDENTU (vzorčni obrazec)

Podatek	Vsebina / Odgovor
ZADEVA	
IBS / PDS / ODU (ime zavezanca)	
SEKTOR	
DATUM IN ČAS NASTANKA INCIDENTA	
DATUM IN ČAS ZAZNAVE INCIDENTA	
OPIS INCIDENTA	
TAKSONOMIJA (klasifikacija)	
OGROŽENA STORITEV	
OCENA STOPNJE NEVARNOSTI	
OCENA MOŽNEGA VPLIVA	
STOPNJA INCIDENTA (C1–C6)	
OPOMBE / DODATNE INFORMACIJE	

Vaja 10: Upravljanje kibernetskih incidentov (preprosta različica)

Namen in cilj

Udeleženci:

- znajo poimenovati **6 faz** (Priprava, Zaznavanje, Zamejitev, Ublažitev, Obnovitev, Zaključek),
- za dan primer znajo izbrati **pravilen naslednji korak**,
- znajo izpolniti **zelo kratek obrazec** o incidentu.

Navodilo za izvedbo

Obkroži faze v pravilnem vrstnem redu:

Priprava → Zaznavanje → Zamejitev → Ublažitev → Obnovitev → Zaključek

Scenarij

Opis dogodka:

V petek ob 10:05 zaposleni poročajo, da je aplikacija za naročila počasna. Ob 10:10 sistemska skrbnica v dnevniku vidi veliko neuspešnih prijav. Ob 10:15 blokira sumljivi IP na požarnem zidu in zamenja geslo storitvenega računa. Ob 11:30 je aplikacija spet normalno dosegljiva. V ponedeljek IT pripravi kratek povzetek, kaj se je zgodilo in kaj bodo izboljšali.

Katera faza je to? (obkroži)

a) "Zaznam veliko neuspešnih prijav." → **Priprava / Zaznavanje / Zaključek**

b) "Začasno blokiram sumljivi IP." → **Zamejitev / Ublažitev / Obnovitev**

c) "Zamenjam geslo in posodobim pravila prijav." → **Ublažitev / Priprava / Zaključek**

d) "Preverim, da aplikacija spet deluje normalno." → **Obnovitev / Zamejitev /**

Zaznavanje

e) "Zapišem, kaj smo se naučili, in dodam ukrepe za naprej." → **Zaključek / Ublažitev / Priprava**

Mini kontrolni seznam (obkljukaj ✓ ali pusti prazno)

Priprava: ☐ imamo seznam ključnih kontaktov ☐ imamo plan za hitri odziv

Zaznavanje: ☐ znamo prepoznati "neuspešne prijave" kot opozorilo

Zamejitev: ☐ začasno omejimo vir napada (npr. blok IP)

Ublažitev: ☐ spremenimo gesla ☐ posodobimo pravila prijav/MFA

Obnovitev: ☐ preverimo delovanje ☐ spremljamo 24 h po obnovi

Zaključek: ☐ zapišemo 3 izboljšave ☐ posodobimo navodila

Mikro obrazec

- **Zadeva:** _____
- **Kdaj zaznano:** _____ ob _____
- **Kratek opis (1–2 stavka):**

_____

- **Kateri hitri ukrep:** _____
- **Katera faza je naslednja:**

_____

Univerzitetna založba
Univerze v Mariboru

5 Rešitve

5.1 Vaja 1

Vrsta incidenta: **2 – Zlonamerna koda**

Glavni učinek: **Razpoložljivost** (sekundarno tudi celovitost, če je prišlo do sprememb datotek)
Utemeljitev (primer):

Incident vključuje delovanje zlonamerne programske kode (trojanec), ki je vplivala na delovanje *WMS* sistema, povzročila zastoje in izbris logov. Ker gre za aktivno škodljivo kodo, dogodek spada v kategorijo "zlonamerna koda". Glavni učinek je bila začasna izguba razpoložljivosti sistema in možnost izgube podatkov.

5.2 Vaja 2

Vrsta incidenta: 8 – **Goljufije** (sekundarno: 3 – zbiranje informacij)

Prizadeti cilj: **Zaupnost** (kraja poverilnic, podatkov za prijavo)

Utemeljitev:

Napadalec je uporabil lažno elektronsko sporočilo, s katerim je pridobil zaupne podatke za prijavo v bančni sistem. To je socialni in finančni napad, zato spada v kategorijo "goljufije". Glavni prizadeti cilj je zaupnost informacij (gesla, finančni podatki).

Predlagani ukrepi:

- uvedba dvostopenjske overitve za dostop do bančnih računov,
- redno ozaveščanje zaposlenih o *phishing* tehnikah in preverjanju povezav.

5.3 Vaja 3

Primer	Pravilna klasifikacija	Utemeljitev (primer)	Tipičen odziv
A	Lažji incident	Grožnja je bila samodejno zaznana in odstranjena, brez vpliva na poslovanje.	Prijava v register dogodkov, analiza vzorca, izobraževanje uporabnika.
B	Težji incident	Neavtoriziran dostop, manjši vpliv na poslovanje (delna izguba podatkov, nekaj naročil).	Izolacija računa, forenzična analiza, obvestilo varnostnemu koordinatorju v 4 h.
C	Kritični incident	Celoten izpad poslovnih procesov, visoka finančna škoda, izguba podatkov.	Aktivacija kriznega načrta, obveščanje vodstva, NOKI poročilo v 1 h, vzpostavitev krizne komunikacije.

5.4 Vaja 4

Primer	Žrtev	Učinek	Utemeljitev
A	Posamezniki (zaposleni)	Kraja osebnih podatkov	Napadalec je pridobil osebne podatke zaposlenih, kar vpliva na zaupnost in zasebnost.
B	Organizacija (dobavitelj in glavno podjetje)	Motnja poslovanja / veriga oskrbe	Incident vpliva na poslovne procese in logistično verigo, povzroči zamude in gospodarsko škodo.
C	Stranke in širša javnost	Izguba ugleda / zaupanja	Zaradi razkritja osebnih podatkov strank podjetje izgubi ugled in poslovne partnerje.

5.5 Vaja 5

Kazalniki učinka (A)

Parameter učinka	Opis dogodka	Stopnja ogroženosti
Razpoložljivost	2 uri izpada storitve	SREDNJA
Zaupnost	Kraja osebnih podatkov 12.000 strank	ZELO VISOKA
Celovitost	Podatki niso spremenjeni, le kopirani	NIZKA
Moteno delovanje	Kratek izpad *ERP/WMS*, začasna nedosegljivost	SREDNJA
Finančna škoda	Stroški forenzike in obveščanja strank	SREDNJA
SKUPNA ocena učinka		VISOKA / ZELO VISOKA

Kazalniki vpliva (B)

Parameter vpliva	Opis dogodka	Stopnja vpliva
Število prizadetih uporabnikov	12.000 strank	VISOKA
Prekinitev storitve	2 uri motenj, nato obnovitev	SREDNJA
Posledice za funkcije	Ni vpliva na kritično infrastrukturo, vpliv na poslovne storitve	SREDNJA
Medresorski učinki / ugled	Medijska objava, pritožbe, izguba zaupanja	VISOKA
Varnost države / državljanov	Ni neposrednega vpliva	NEZNATNA
SKUPNA ocena vpliva		VISOKA

Določitev končne stopnje incidenta

Kombinacija učinka in vpliva	Končna stopnja incidenta	Prag poročanja
Učinek: ZELO VISOKA / VISOKA + Vpliv: VISOKA	Težji incident – nad pragom	Obvezno poročanje (npr. C3 ali višje)

Utemeljitev

Incident vključuje krajo osebnih podatkov velikega števila uporabnikov (visoka stopnja učinka na zaupnost) in vpliva na več tisoč strank (visoka stopnja vpliva).

Čeprav ni prizadeta kritična infrastruktura, je zaradi obsega in vrste podatkov incident nad pragom obveznega poročanja. Potrebno je obvestiti nacionalni CSIRT/SI-CERT in informacijsko pooblaščenko (zaradi GDPR).

5.6 Vaja 6

Primer	Pravilna stopnja	Obvezno obveščanje	Utemeljitev
A	C3 – Pomemben incident	Zavezanec → SI-CERT / SIGOV-CERT → PNO	Napad na spletne storitve državnega organa vpliva na več uporabnikov in ima javni vpliv, zato gre za pomemben incident, ki se prijavi brez odlašanja.
B	C2 – Zelo pomembeni incident	Zavezanec → SI-CERT / SIGOV-CERT + obveščanje PNO	Incident prizadene bistveno infrastrukturo (zdravstvene dobave), ima velik vpliv na delovanje kritičnih sistemov, zato je nad pragom C2.
C	C6 – Varnostni dogodek (grožnja)	Interno beleženje, po potrebi SI-CERT	Poskus brez posledic; dogodek se zabeleži, a ne zahteva formalnega poročanja.

5.7 Vaja 7

Element	Odgovor
Zavezanec / prijavitelj	Logistično podjetje (kot zavezanec po ZInfV)
Koga mora obvestiti?	SI-CERT ali SIGOV-CERT (glede na vrsto povezave)
Predlagana stopnja incidenta	C5 – Lažji incident
Utemeljitev	Zaznan je poskus vdora in priprava na napad, brez dejanskega vpliva ali škode. Gre za varnostni dogodek s potencialnim vplivom.
Obvestilo PNO	Da – incident prijavi SI-CERT/SIGOV-CERT, ki o njem obvesti PNO; PNO potrdi stopnjo.

5.8 Vaja 8

Element	Odgovor
Stopnja incidenta	C3 – Pomembni incident
Obveznost poročanja	Da (obvezno)
Začetno poročilo	V 24 urah od zaznave incidenta
Vmesno poročilo	V 72 urah od zaznave ali po potrebi
Končno poročilo	Po zaključku incidenta (najpozneje v nekaj dneh)
Utemeljitev	Napad ima vpliv na delovanje bistvene storitve (elektronska pošta podjetja, ki opravlja logistične storitve za državo). Gre za srednje močan vpliv, zato spada med pomembne incidente (C3). Po ZInfV je obvezno poročanje SI-CERT ali SIGOV-CERT.

5.9 Vaja 9

Podatek	Primer pravilne vsebine
ZADEVA	Neavtoriziran dostop do strežnika e-naročanja – TransLog d.o.o.
IBS / PDS / ODU	TransLog d.o.o.
SEKTOR	Logistika in oskrbovalne verige (izvajalec bistvenih storitev)
DATUM IN ČAS NASTANKA INCIDENTA	25. 10. 2025 ob 08:30
DATUM IN ČAS ZAZNAVE INCIDENTA	25. 10. 2025 ob 08:40
OPIS INCIDENTA	Zaznan nepooblaščen dostop iz tujine, uspešna prijava v sistem e-naročanja. Sistem odklopljen, izvedena menjava gesel in analiza logov.
TAKSONOMIJA (klasifikacija)	Poskus vdora / nepooblaščen dostop
OGROŽENA STORITEV	Portal za e-naročanje (ERP-modul)
OCENA STOPNJE NEVARNOSTI	Visoka – možnost kraje poslovnih podatkov
OCENA MOŽNEGA VPLIVA	Srednji – začasna prekinitev storitve, vpliv na državni oskrbovalni proces
STOPNJA INCIDENTA (C1–C6)	C3 – Pomembni incident
OPOMBE	Incident prijavljen SI-CERT 25.10. ob 09:15 po telefonu, poročilo poslano isti dan.

5.10 Vaja 10

1. vrstni red:

Priprava → Zaznavanje → Zamejitev → Ublažitev → Obnovitev → Zaključek

3. a) **Zaznavanje** b) **Zamejitev** c) **Ublažitev** d) **Obnovitev** e) **Zaključek**

4. kontrolni seznam: cilj je vsaj po eno ✓ pri vsaki fazi.

5. primer:

- Zadeva: "Neuspešne prijave in upočasnitev aplikacije"
- Kdaj?: "petek, 10:10"
- Opis: "Povečan poskus prijav, kratka upočasnitev."
- Hitri ukrep: "blok sumljivega IP"
- Naslednja faza: "Ublažitev (zamenjava gesel, MFA pravila)"

Univerzitetna založba
Univerze v Mariboru

6 Sklep

Teoretično razumevanje kibernetskega področja se je skozi poglavje potrdilo kot temelj kibernetske varnosti in obrambe. Kibernetski prostor je osrednje okolje sodobnih družbenih, gospodarskih in mednarodnih interakcij, zato zahteva nenehno prilagajanje ter razvoj učinkovitih strategij za svoje varovanje. Spoznali smo, da ga različne institucije opredeljujejo različno, da ga sestavljajo fizična, logična in človeška razsežnost ter da zaradi globalnosti, asimetričnosti in horizontalnosti ne pozna geografskih in časovnih meja. Prav te lastnosti pojasnjujejo, zakaj se lahko napad na informacijski sistem organizacije začne kjerkoli in kadarkoli ter zakaj je njegovo razumevanje nujno tudi za strokovnjake s področja logistike, katerih delo v celoti teče po digitalnih poteh.

Pregled razmerij med pojmi varovanja kibernetskega prostora je pokazal, da je jasna in usklajena terminologija temelj učinkovite zaščite digitalnih infrastruktur. Razlikovanje med informacijsko zagotovitvijo, informacijsko varnostjo, kibernetsko varnostjo in kibernetsko obrambo ni zgolj akademsko vprašanje, ampak praktična potreba, ki omogoča, da se s kibernetskimi grožnjami uspešno soočajo vse ravni družbe, od posameznih uporabnikov do vladnih organov in podjetij. Enotno razumevanje pojmov izboljšuje komunikacijo in sodelovanje med deležniki, kar je v oskrbovalnih verigah, kjer sodeluje veliko partnerjev z različnim predznanjem, še posebej dragoceno.

Kibernetske grožnje obsegajo vse od zlonamernih napadov in vdorov do nezakonitega razkrivanja informacij in sabotaž, njihova primerjava po Svetetovem modelu pa je razkrila, da obravnavani dokumenti pretežno opredeljujejo namerne človeške dejavnike, premalo pozornosti pa namenjajo višji sili ter pomanjkljivostim strojne in programske opreme. Za logistične organizacije je to pomembno opozorilo, saj oskrbovalno verigo enako učinkovito ustavijo tudi nenamerne napake in odpovedi opreme. Analize ENISE poleg tega kažejo, da med najresnejše grožnje prihodnosti sodijo prav napadi na dobavne verige,

zato se morajo podjetja na grožnje pripravljati sistematično, s stalno budnostjo, posodabljanjem tehnologij in usposabljanjem zaposlenih.

Primerjava med Natom in EU razkriva različna, a dopolnjujoča se pristopa. Nato se osredotoča na kolektivno obrambo, operativno odzivanje in odpornost zavezništva, kar prek članstva zavezuje tudi Slovenijo in njen obrambni sistem. EU deluje predvsem regulativno in naložbeno, s poudarkom na zakonodaji, certificiranju, izobraževanju in raziskavah. Za logistiko sta pomembna oba okvira. Natova odpornost temelji tudi na zanesljivem delovanju prometa in oskrbe, ki ju zagotavlja civilni sektor, evropska pravila pa promet uvrščajo med sektorje visoke kritičnosti in podjetjem prinašajo tako obveznosti kot priložnosti, od enotnih pravil čezmejnega poslovanja do sredstev za dvig kibernetske odpornosti.

Univerzitetna založba
Univerze v Mariboru

Viri

Aiyanyo, D., Hamman, S. in Heuiseok, L. (2020). A systematic review of defensive and offensive cybersecurity with machine learning. Applied Sciences, 10(17). https://www.mdpi.com/2076-3417/10/17/5811

Andronache, A. in Althonayan, A. (2018). Shifting from information security towards a cybersecurity paradigm. University of Salford, ICIME Conference.

ARNES. (2023a). Poročilo o kibernetski varnosti za leto 2022. Nacionalni odzivni center za kibernetsko varnost SI-CERT, Akademska in raziskovalna mreža Slovenije.

ARNES. (2023b). Prijava incidenta. https://www.cert.si/prijava-incidenta/

ARNES. (2023c). O projektu. https://www.varninainternetu.si/kdo-smo/

ARNES. (2023e). O centru SI-CERT. https://www.cert.si/o-nas/

ARNES. (2025). Poročilo o kibernetski varnosti za leto 2024. Nacionalni odzivni center za kibernetsko varnost SI-CERT, Akademska in raziskovalna mreža Slovenije. https://www.cert.si/wp-content/uploads/2025/08/Porocilo-o-kibernetski-varnosti_SI-CERT_2024.pdf

CyberTalk.org. (2024). What is cyber defense? https://www.cybertalk.org/what-is-cyber-defense/

Dalmjin, A., Banse, V., Lumiste, L., Teixeira, J. in Balci, A. (ur.). (2020). Cyber commanders' handbook. NATO Cooperative Cyber Defence Centre of Excellence.

Ducheine, P., Haaster, J. v. in Harskamp, R. v. (2017). Manoeuvring and generating effects in the information environment (Amsterdam Law School Legal Studies Research Paper No. 2017-30). Amsterdam Center for International Law, University of Amsterdam.

Dunn, M. in Wigert, I. (2004). International CIIP handbook 2004. http://e-collection.ethbib.ethz.ch/eserv/eth:31123/eth-31123-02.pdf

Dutta, S. in Lanvin, B. (2020). The Network Readiness Index 2020: Accelerating digital transformation in a post-COVID global economy. Portulans Institute.

ENISA. (2017). ENISA overview of cybersecurity and related terminology, version 1. European Union Agency for Network and Information Security.

ENISA. (2022). Threat landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

ENISA. (2023a). About ENISA – The European Union Agency for Cybersecurity. https://www.enisa.europa.eu/about-enisa

ENISA. (2023b). European Cybersecurity Month. https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/european-cyber-security-month

ENISA. (2023c). Identifying emerging cyber security threats and challenges for 2030. https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

EU. (2022). A strategic compass for security and defence. https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

EU. (2023b). Akt EU o kibernetski solidarnosti. https://digital-strategy.ec.europa.eu/sl/policies/cyber-solidarity

EU. (2023c). The European Cybersecurity Competence Centre. https://cybersecurity-centre.europa.eu/index_en

Evropska komisija. (2023a). Direktiva o ukrepih za visoko skupno raven kibernetske varnosti v Uniji. https://digital-strategy.ec.europa.eu/sl/policies/nis2-directive

Evropska komisija. (2023b). Akt o kibernetski odpornosti. https://digital-strategy.ec.europa.eu/sl/library/cyber-resilience-act

Evropska komisija. (2023c). Akt EU o kibernetski varnosti. https://digital-strategy.ec.europa.eu/sl/policies/cybersecurity-act

Evropska komisija. (2023d). Horizon Europe. https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/horizon-europe_en

Evropska komisija. (2023e). Cybersecurity policies. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

Evropska komisija. (2023f). Strategija za kibernetsko varnost. https://digital-strategy.ec.europa.eu/sl/policies/cybersecurity-strategy
Evropska komisija. (2023g). The Digital Europe Programme. https://digital-strategy.ec.europa.eu/en/activities/digital-programme
Evropska komisija. (2023h). What's next? The InvestEU Programme (2021–2027). https://ec.europa.eu/commission/priorities/jobs-growth-and-investment/investment-plan-europe-juncker-plan/whats-next-investeu-programme-2021-2027_en
Evropska komisija. (2023i). Joint Cyber Unit. https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit
Evropska komisija. (2023j). Cybersecurity of 5G networks – EU toolbox of risk mitigating measures. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
Evropska komisija. (2023k). Digital skills and jobs. https://digital-strategy.ec.europa.eu/en/policies/digital-skills-and-jobs
Evropska komisija. (2023l). Cyber defence: EU boosts action against cyber threats. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642
Evropska unija. (2023). Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises. https://eur-lex.europa.eu/eli/reco/2017/1584/oj
Furlan, B. (2021). Vojaška strategija. Center vojaških šol.
Gay, S., Suret, J.-F., Virvilis-Kollitiris, N. in Hallingstad, G. (2016). CIS security capability target ambition assessment (Technical Report 2014/NCB009779/02). NATO Communications and Information (NCI) Agency.
ISO/IEC. (2020). ISO/IEC TS 27100:2020. Information technology – Cybersecurity – Overview and concepts. ISO/IEC.
ITU. (2021). Global Cybersecurity Index 2020: Measuring commitment to cybersecurity. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
Kavčič, M. (2018). Ocena kibernetskih tveganj. Ministrstvo za javno upravo.
Kavčič, M. (2023). Sistem kibernetske varnosti Slovenije. Ministrstvo za javno upravo.
Kazenski zakonik (KZ-1). (2023). Uradni list RS, št. 50/12 s spremembami. http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5050
Maconachy, W. V., Schou, C. D., Ragsdale, D. in Welch, D. (2021). A model for information assurance: An integrated approach. https://www.researchgate.net/publication/235470635
Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S. in Frye, J. (2021). Cyber threat metrics. Sandia National Laboratories.
Maurer, T. in Morgus, R. (2014). Compilation of existing cybersecurity and information security related definitions. Harvard University, New America.
McCargo, H. (2020). Cyber defense vs. cyber security (key differences to know!). https://www.uscybersecurity.com/blogs/cyber-defense-vs-cyber-security-key-differences-to-know
Ministrstvo za digitalno preobrazbo. (2023). Kvalificirano digitalno potrdilo. https://e-uprava.gov.si/si/podrocja/osebni-dokumenti-potrdila-selitev/osebni-dokumenti/digitalno-potrdilo-za-elektronsko-poslovanje
MORS. (2008). Pravilnik o varovanju komunikacijskega in informacijskega sistema Ministrstva za obrambo Republike Slovenije (št. 007-161/2008-2 z dne 12. 6. 2008). Ministrstvo za obrambo RS.
NATO. (2006). Riga Summit Declaration (Press Release (2006) 150). https://www.nato.int/cps/en/natohq/official_texts_37920.htm
NATO. (2008). Bucharest Summit Declaration (Press Release (2008) 049). https://www.nato.int/cps/en/natohq/official_texts_8443.htm
NATO. (2009). Strasbourg/Kehl Summit Declaration (Press Release (2009) 044). https://www.nato.int/cps/en/natohq/news_52837.htm
NATO. (2010). Lisbon Summit Declaration (Press Release (2010) 155). https://www.nato.int/cps/en/natohq/official_texts_68828.htm
NATO. (2012). Chicago Summit Declaration (Press Release (2012) 062). https://www.nato.int/cps/en/natohq/official_texts_87593.htm
NATO. (2014a). NATO cyber defence taxonomy and definitions (AC/322-N(2014)0072). NATO.
NATO. (2014b). Wales Summit Declaration (Press Release (2014) 120). https://www.nato.int/cps/en/natohq/official_texts_112964.htm
NATO. (2016a). Warsaw Summit Communiqué (Press Release (2016) 100). https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO. (2016b). Cyber Defence Pledge (Press Release (2016) 124). https://www.nato.int/cps/en/natohq/official_texts_133177.htm
NATO. (2018a). Allied joint doctrine for communication and information systems (AJP-6(A), ver. 1). NATO.
NATO. (2018b). Brussels Summit Declaration (Press Release (2018) 074). https://www.nato.int/cps/en/natohq/official_texts_156624.htm
NATO. (2018c). High level taxonomy of cyberspace operations. NATO.
NATO. (2019a). Technical and implementation directive on CIS security (AC/322-D/0048-REV3 (INV)). NATO.
NATO. (2019b). Draft proposal for a cyber incident taxonomy (AC/322(CP/4)N(2019)0032-REV2 (INV)). NATO.
NATO. (2020). Allied joint doctrine for cyberspace operations (Edition A, Version 1, NATO Standard). NATO.
NATO. (2021). Brussels Summit Communiqué (Press Release (2021) 086). https://www.nato.int/cps/en/natohq/news_185000.htm
NATO. (2022). Madrid Summit Declaration (Press Release (2022) 095). https://www.nato.int/cps/en/natohq/official_texts_196951.htm
NATO. (2023). Vilnius Summit Communiqué (Press Release (2023) 001). https://www.nato.int/cps/en/natohq/official_texts_217320.htm
NATO. (2024). Washington Summit Declaration (Press Release (2024) 001). https://www.nato.int/cps/en/natohq/official_texts_227678.htm
NIST. (2003). NIST Special Publication 800-59: Information security. National Institute of Standards and Technology.
NIST. (2012). NIST Special Publication 800-30. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
Odlok o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za informacijsko varnost. (2021). Uradni list RS, št. 180/21. http://www.pisrs.si/Pis.web/pregledPredpisa?id=ODLO2534
OED. (2024). Oxford English Dictionary. https://www.oed.com/search/dictionary/?scope=Entries&q=information%20security
Oxford University Press. (2023). Oxford Learner's Dictionaries. https://www.oxfordlearnersdictionaries.com/
Paulsen, C. in Byers, R. (2019). Glossary of key information security terms (NISTIR 7298, Revision 3). https://doi.org/10.6028/NIST.IR.7298r3
Plevnik, M. in Ščavničar, D. (2026). Kibernetski prostor in Slovenska vojska: visokošolski učbenik za vojaško izobraževanje in usposabljanje. Ministrstvo za obrambo Republike Slovenije, Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje. https://dk.mors.si/IzpisGradiva.php?id=1666
Računsko sodišče. (2021). Revizijsko poročilo: Učinkovitost zagotavljanja kibernetske varnosti v Republiki Sloveniji. Računsko sodišče RS.
Reid, R. in Van Niekerk, J. (2014). From information security to cyber security cultures. https://digifors.cs.up.ac.za/issa/2014/Proceedings/Full/42_Paper.pdf
Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-2). (2019). Uradni list RS, št. 59/19. http://www.pisrs.si/Pis.web/pregledPredpisa?id=RESO124
Rouse, M. (2024). Cyber defense. https://www.techopedia.com/definition/6705/cyber-defense
Santos, O. (2020). Cisco CyberOps Associate CBROPS 200-201 official cert guide. Cisco Press.
Sklep o dopolnitvi Sklepa o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov. (2017). Uradni list RS, št. 17/17. https://www.uradni-list.si/glasilo-uradni-list-rs/celotno-kazalo/201717
Solms, B. in Solms, R. (2018). Cybersecurity and information security – what goes where? Information and Computer Security, 26(1). https://doi.org/10.1108/ICS-04-2017-0025
Svete, U. (2007). Informacijsko ogrožanje nacionalne varnosti. V I. Prezelj (ur.), Model celovitega ocenjevanja ogrožanja nacionalne varnosti Republike Slovenije. Ministrstvo za obrambo, Direktorat za obrambne zadeve, Sektor za civilno obrambo.
Ulsch, N. M. (2014). Cyber threat! How to manage the growing risk of cyber attacks. Wiley.
Uredba o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev. (2019). Uradni list RS, št. 39/19. http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED7808
URSIV. (2021a). Razglašeno stanje povečane ogroženosti varnosti omrežij in informacijskih sistemov. https://www.gov.si/novice/2021-12-14-razglaseno-stanje-povecane-ogrozenosti-varnosti-omrezij-in-informacijskih-sistemov/
URSIV. (2021b). Kritična ranljivost Microsoft Exchange strežnikov. https://www.gov.si/novice/2021-03-09-kriticna-ranljivost-microsoft-exchange-streznikov/

URSIV. (2023a). Urad Vlade Republike Slovenije za informacijsko varnost. https://www.gov.si/drzavni-organi/vladne-sluzbe/urad-vlade-za-informacijsko-varnost/o-uradu/
URSIV. (2023b). Povabilo k sodelovanju na razpisih EU s področja kibernetske varnosti. https://www.gov.si/zbirke/javne-objave/povabilo-k-sodelovanju-na-razpisih-eu-s-podrocja-kibernetske-varnosti/
URSIV. (2023c). Povabilo k izkazu interesa za vključitev v mrežo srednjih šol za kibernetsko varnost. https://www.gov.si/zbirke/javne-objave/povabilo-za-vzpostavitev-mreze-srednjih-sol-za-kibernetsko-varnost/
URSIV. (2023d). Novice. https://www.gov.si/novice/?org%5B0%5D=2851
URSIV. (2023e). Informacijska varnost. https://www.gov.si/teme/informacijska-varnost/
U.S. Department of Defense. (2018). Cyberspace operations (Joint Publication 3-12). https://irp.fas.org/doddir/dod/jp3_12.pdf
Vlada RS. (2016a). Strategija kibernetske varnosti: vzpostavitev sistema zagotavljanja visokega nivoja kibernetske varnosti. https://www.gov.si/assets/ministrstva/MDP/DID/Strategija-kibernetske-varnosti.pdf
Vlada RS. (2021). Nacionalni načrt odzivanja na kibernetske incidente (NOKI). https://www.gov.si/assets/URSIV/Nacionalni-nacrt-odzivanja-na-kibernetske-incidente.pdf
Vlada RS. (2024a). Obrambna strategija Republike Slovenije. https://www.gov.si/assets/ministrstva/MO/Dokumenti/OS_8n_sprejeta_24_4_2024.pdf
Vlada RS. (2024b). Vojaška strategija Republike Slovenije. Vlada RS. *(dodaj številko dokumenta ali povezavo, če obstaja javna različica)*
Walia, P. (2024). Cyber defense. https://www.merriam-webster.com/dictionary/cyber%20defense
Wang, G. in Wendy, H. (2019). Measuring information security and cybersecurity on private cloud computing. Journal of Theoretical and Applied Information Technology.
Zakon o informacijski varnosti (ZInfV). (2018). Uradni list RS, št. 30/18. https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2018-01-0934
Zakon o informacijski varnosti (ZInfV-1). (2025). Uradni list RS, št. 40/25. https://pisrs.si/pregledPredpisa?id=ZAKO8934

UPRAVLJANJE INFORMATIKE IN INFORMACIJSKE VARNOSTI

MIHAEL PLEVNIK, BORUT JEREB

Univerza v Mariboru, Fakulteta za logistiko, Celje, Slovenija
mihael.plevnik2@um.si, borut.jereb@um.si

"Upravljanje informatike in informacijske varnosti" je gradivo avtorjev Mihaela Plevnika in Boruta Jereba, namenjeno predmetu Informatika in informacijska varnost v organizacijah na Fakulteti za logistiko Univerze v Mariboru. Učbenik na praktičen način predstavi pot informacije v digitalnem okolju organizacij v treh sklopih: delovanje omrežne komunikacije od vpisa spletnega naslova do prikaza strani (DNS, TCP/IP, NAT, ARP, MAC ter diagnostična orodja ping, nslookup, netstat, Wireshark), osnove jezika HTML za strukturiranje in predstavitev vsebin na spletu ter kibernetsko varnost, vključno z ureditvijo na ravni NATO, EU in Slovenije. Vsak sklop združuje teorijo, praktične primere in vaje, sklop o HTML pa se zaključi s samostojno izdelavo spletne strani. Gradivo bodočim logistom ne daje le splošne računalniške pismenosti, temveč razumevanje digitalnega toka informacij, ki spremlja vsako pošiljko, in sposobnost za njegovo osnovno preverjanje ter odgovorno varovanje v oskrbovalnih verigah.

DOI
https://doi.org/10.18690/um.fl.8.2026

ISBN
978-961-299-219-4

Ključne besede:
informatika, informacijska varnost, kibernetska varnost, računalniška omrežja, HTML, logistika

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.fl.8.2026

ISBN
978-961-299-219-4

Keywords:
informatics,
information security,
cybersecurity,
computer networks
HTML,
logistics

MANAGING INFORMATICS AND INFORMATION SECURITY

MIHAEL PLEVNIK, BORUT JEREB

University of Maribor, Faculty of Logistics, Celje, Slovenia
mihael.plevnik2@um.si, borut.jereb@um.si

"Managing Informatics and Information Security" is a set of course materials by Mihael Plevnik and Borut Jereb for the course Informatics and Information Security in Organizations at the Faculty of Logistics, University of Maribor. In three thematic units, the textbook illustrates, in a hands-on way, the journey of information through an organization's digital environment: network communication from typing a web address to displaying the page (DNS, TCP/IP, NAT, ARP, MAC, and diagnostic tools such as ping, nslookup, netstat, and Wireshark), the basics of HTML for structuring and presenting web content, and cybersecurity, including regulation at the NATO, EU, and Slovenian levels. Each unit combines theory, practical examples, and exercises, with the HTML unit culminating in building a website independently. The material gives future logistics professionals more than general computer literacy: an understanding of the digital information flow behind every shipment, and the ability to check and responsibly safeguard it across supply chains.

University of Maribor Press



Univerza v Mariboru

Fakulteta za logistiko