

Praksa - Zaščita OS

Vrste okužb računalnika:

- Kaj je zlonamerna programska oprema (malware)?
- Naštej in opiši zlonamerno programsko opremo.

Izbira protivirusne zaščite:

- Kaj je protivirusna programska oprema („Offline“, „Cloud“)?
- Naštej 5 vrst protivirusne programske opreme (Windows, Linux OS).



Praksa - Zaščita OS

Preprečevanje okužb:

- Posodobljen operacijski sistem (varnostni popravki)
- Posodobljena protivirusna oprema (definicija)
- Namestitev požarnega zidu (vrata, protokoli)
- Namestitev aplikacij za preprečevanje nezaželenne pošte (AntiSpam filtri)



Praksa - Zaščita OS

Nameščanje in upravljanje zaščite:

Windows OS: GUI

- V operacijskem sistemu Windows, odpri aplikacijo „Windows Defender Antivirus” oziroma „Zaščita pred virusi in grožnjami”. Posodobi protivirusni program. V nastavitvah spremeni: Zaščita pred virusi in grožnjami --> upravljanje nastavitev --> izklopi prve 3 funkcije. Iz mrežne mape prenesi datoteko „Test Virus.7z” in jo shrani na namizje (razširi v mapo). V nastavitvah protivirusne opreme, spremeni: Zaščita pred virusi in grožnjami --> upravljanje nastavitev --> Vklopi sprotno zaščito. S protivirusnim programom preglej vsako datoteko posebej in dokumentiraj ali protivirusna aplikacija zazna okužbo (najdene okužbe lahko preveriš še v log datoteki oz. v nastavitvah protivirusnega programa). Postopek vaje dokumentiraj oz. shrani zaslonske slike.



Praksa - Zaščita OS

Nameščanje in upravljanje zaščite:

Windows OS: GUI

- Odstrani oz. izklopi že nameščeno protivirusno programsko opremo. Namesti eno od prej naštetih protivirusnih programov (Avast, AVG, Avira, ESET ali ClamWin) in ga zaženi. Posodobi protivirusni program. V nastavitvah izključi sprotno zaščito. Iz mrežne mape prenesi datoteko „Test Virus.7z” in jo shrani na namizje (razširi v mapo). V nastavitvah protivirusne opreme, vključi sprotno zaščito. S protivirusnim programom preglej vsako datoteko posebej in dokumentiraj ali protivirusna aplikacija zazna okužbo (najdene okužbe lahko preveriš še v log datoteki oz. v nastavitvah protivirusnega programa). Postopek vaje dokumentiraj oz. shrani zaslonske slike. Odstrani nameščeno protivirusno opremo.



Praksa - Zaščita OS

Nameščanje in upravljanje zaščite:

Windows OS: CMD

- V operacijskem sistemu Windows, odpri aplikacijo CMD kot administrator. V ukazni vrstici odpri mapo, v kateri je nameščen „Windows Defender Antivirus“ (C:\Program Files\Windows Defender).
- Protivirusni program, najprej izključi (sc -?; sc -h): „sc config WinDefend start= disabled“, „sc stop WinDefend“, „sc query WinDefend“. Iz mrežne mape prenesi datoteko „Test Virus.7z“ in jo shrani na namizje (razširi v mapo).
- Protivirusni program vključi: „sc config WinDefend start= auto“, „sc start WinDefend“, „sc query WinDefend“.



Praksa - Zaščita OS

Nameščanje in upravljanje zaščite:

Windows OS: CMD

- Posodobi protivirusni program:
"%ProgramFiles%\Windows Defender\MpCmdRun.exe" -
SignatureUpdate
- S protivirusnim programom preglej vsako datoteko posebej in dokumentiraj ali protivirusna aplikacija zazna okužbo (najdene okužbe lahko preveriš še v log datoteki oz. v nastavitvah protivirusnega programa). Postopek vaje dokumentiraj oz. shrani zaslonske slike.



Praksa - Zaščita OS

Nameščanje in upravljanje zaščite:

Linux OS: GUI

- V operacijskem sistemu Linux, s pomočjo aplikacije „Ubuntu Software“, namesti protivirusno programsko opremo „ClamTK“.
- Iz spletne strani „www.eicar.org --> download --> HTTP/S --> eicar.com, [eicar.com.txt](#), [eicar_com.zip](#), [eicarcom2.zip](#)“, prenesi omenjene datoteke in jih shrani na namizje.
- Odpri protivirusni program in ga posodobi.



Praksa - Zaščita OS

Nameščanje in upravljanje zaščite:

Linux OS: GUI

- S protivirusnim programom preglej vsako datoteko posebej in dokumentiraj ali protivirusna aplikacija zazna okužbo (najdene okužbe lahko preveriš še v log datoteki oz. v nastavitvah protivirusnega programa). Postopek vaje dokumentiraj oz. shrani zaslonske slike. Odstrani nameščeno protivirusno opremo.



VEGOVA

ELEKTROTEHNIŠKO-RAČUNALNIŠKA
STROKOVNA ŠOLA IN GIMNAZIJA
LJUBLJANA

Praksa - Zaščita OS

Nameščanje in upravljanje zaščite:

Linux OS: CLI

- V operacijskem sistemu Linux, s pomočjo ukazne vrstice, namesti protivirusno programsko opremo „clamav“.
- Iz spletne strani „www.eicar.org --> download --> HTTP/S --> eicar.com, eicar.com.txt, eicar_com.zip, eicarcom2.zip“, prenesi omenjene datoteke in jih shrani na namizje: „[/home/uporabnik/Desktop](https://home/uporabnik/Desktop)“.
- Protivirusni program posodobi.



VEGOVA

ELEKTROTEHNIŠKO-RAČUNALNIŠKA
STROKOVNA ŠOLA IN GIMNAZIJA
LJUBLJANA

Praksa - Zaščita OS

Nameščanje in upravljanje zaščite:

Linux OS: CLI

- S protivirusnim programom preglej vsako datoteko posebej in dokumentiraj ali protivirusna aplikacija zazna okužbo (najdene okužbe lahko preveriš še v log datoteki oz. v nastavitvah protivirusnega programa). Postopek vaje dokumentiraj oz. shrani zaslonske slike. Odstrani nameščeno protivirusno opremo.



VEGOVA

ELEKTROTEHNIŠKO-RAČUNALNIŠKA
STROKOVNA ŠOLA IN GIMNAZIJA
LJUBLJANA