

Национални ЦЕРТ – осврт на активности и перспектива даљег развоја информационе безбедности

др Марко Крстић, руководилац Службе за
информациону безбедност и послове
Националног ЦЕРТ-а, РАТЕЛ



Садржај

- преглед стања у Републици Србији у 2022. години
- превентивне и проактивне активности Националног ЦЕРТ-а
- едукација и подизање свести из области информационе безбедности
- очекиване надлежности у складу са Нацртом Закона о информационој безбедности

Преглед стања у Републици Србији у 2022. години



Преглед стања у Републици Србији у 2022. години



Преглед стања у Републици Србији у 2022. години

5 најчешће пријављених инцидената у 2022. години



Превентивне и проактивне активности Националног ЦЕРТ-а



Дељење информација о претњама и ризицима

- успостављена МИСП платформа за размену информација о претњама и ризицима за ЦЕРТ-ове самосталних оператора и Посебне ЦЕРТ-ове
- доступни подаци који се размењују у оквиру FIRST организације која окупља преко 600 ЦЕРТ-ова из целог света
- ради се на изради материјала у циљу едукације корисника и на размени података са Посебним ЦЕРТ-овима како би се добиле информације о претњама и ризицима везаним за територију Републике Србије



Рана упозорења

- повећан број извора података
- више није проблем недовољна количина података већ се јавља проблем превелике количине података
- предвиђен развој система за консолидацију прикупљених података и портала помоћу кога би оператори ИКТ система могли да прате информације везане за њихову организацију

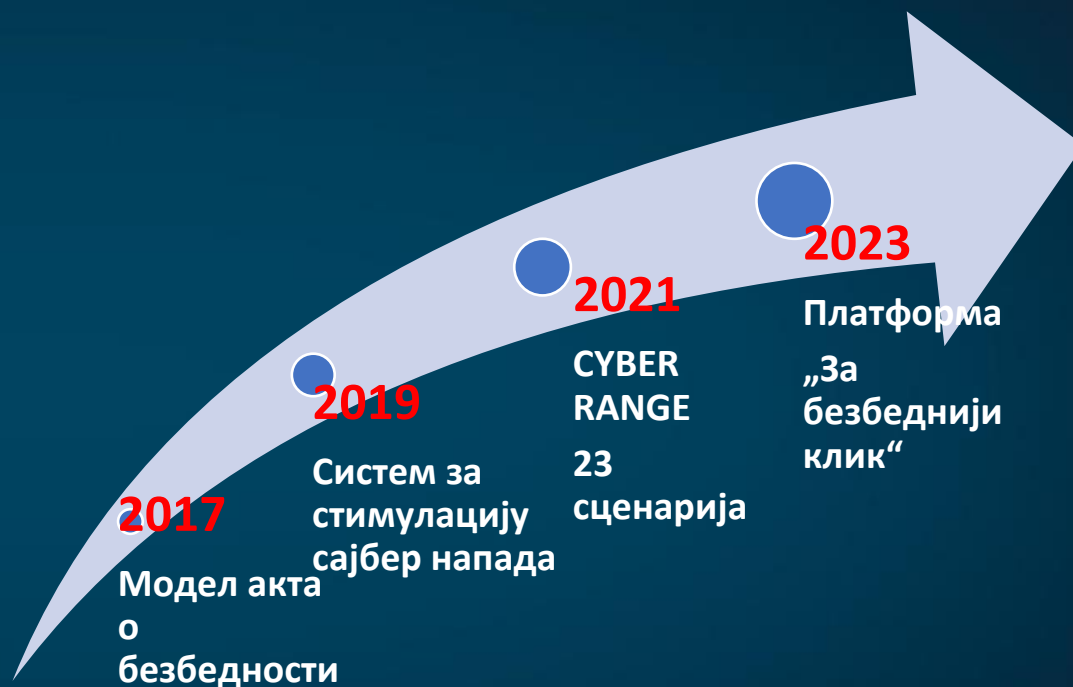


Едукација и подизање свести из области информационе безбедности



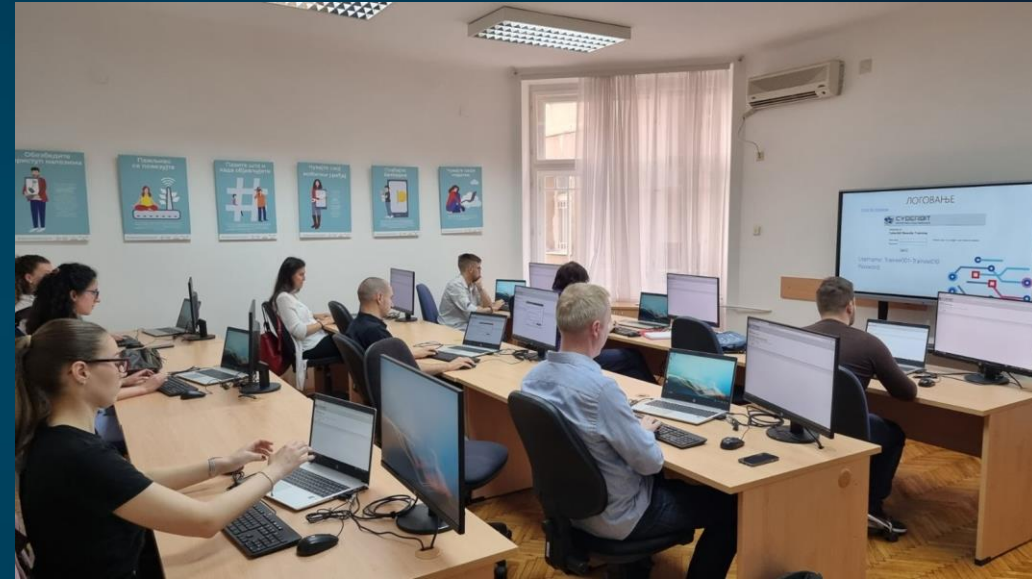
Едукација и подизање свести из области информационе безбедности

- Разумевање технологије
- Имплементација мера заштите
- Унапређење вештина и подизање нивоа знања
- Детекција и реакција на критичне безбедносне активности



Едукација и подизање свести из области информационе безбедности (Cyber range)

- настављена сарадња са НАЛЕД-ом у циљу обуке запослених у локалним самоуправама
- успостављена сарадња са ФИН-ЦЕРТ-ом у циљу обуке запослених у финансијском сектору
- очекујемо да обука буде доступна путем НАЈУ од следеће године за све државне службенике



Едукација и подизање свести из области информационе безбедности (платформа за безбеднији клик)

The image displays a grid of 10 educational cards, each with a title, a brief description, and a 'Почни сада' (Start now) button. The cards are arranged in three rows: the first two rows have four cards each, and the third row has two cards. Each card includes a small icon, a date in the top right corner, and engagement statistics (likes and shares) in the bottom left corner.

- Ажурирање/Update** (Јуни): Значај ажурирања оперативних система, софтвера и апликација. 1 like, 2m shares, 400 likes.
- Заштита мобилних телефона** (Јуни): Основне информације о заштити мобилних телефона. 1 like, 5m shares, 400 likes.
- Критична инфраструктура** (Април): Значај заштите критичне инфраструктуре. 1 like, 400 likes.
- Фишинг** (Децембар): Фишинг је најзаступљенији тип сајбер напада. 2 likes, 800 likes.
- Креирање и безбедност лозинки** (Новембар): Креирање и управљање лозинкама на безбедан начин. 5 likes, 12m shares, 100 likes.
- Безбедност на друштвеним мрежама** (Новембар): Важност заштите наших личних података приликом коришћења друштвених мрежа. 4 likes, 16m shares, 400 likes.
- Рансомвер** (Децембар): Ближе упознавање корисника са Рансомвер типом сајбер напада. 1 like, 20m shares, 400 likes.
- Креирање резервних копија** (Децембар): Упознавање са основним предностима које нуде резервне копије важних датотека, ако дође до хакерског напада. 1 like, 20m shares, 400 likes.
- Социјални инжењеринг** (Децембар): Социјални инжењеринг је усмерен на... 1 like, 20m shares, 400 likes.
- Безбедно коришћење отвореног бежичног интернета (Wi-Fi)** (Децембар): 1 like, 20m shares, 400 likes.

<https://learn.cert.rs/>

Очекиване надлежности у складу са Нацртом Закона о информационој безбедности



Очекиване надлежности у складу са Нацртом Закона о информационој безбедности


- помоћ у праћењу стања безбедности ИКТ система у реалном или приближно реалном времену на захтев оператора ИКТ система од посебног значаја
- проактивно скенирање ИКТ система, на захтев оператора ИКТ система од посебног значаја, у циљу откривања рањивости које могу потенцијално да значајно наруше безбедност
- координатор за потребе координисаног откривања рањивости

Хвала на пажњи



Национална сајбер конференција 2023.

Информациона безбедност
- заједничка одговорност

 Уторак
17. октобар
Београд

 Хотел
Crowne Plaza
& Онлајн

