

Сајбер криминал и мере заштите

Семинарски рад у оквиру курса Техничко и научно писање

Богдан Мицић,
Никола Милорадовић,
Исидора Перовић,
Филип Антанасковић

Математички факултет
Универзитет у Београду

10.12.2022.

Литература

- В. Кораћ, Д. Прља, А. Дилигенски, *Дигитална форензика*, Београд 2016.
- Сајбер тероризам као окидач све интензивније потребе за безбедност система од опасности које долазе са интернета, Сандра Клисарић, 2021.
- Eric Cole, *How to secure your company*, Computerworld, 2016.
- Ханипот и где се користи, <https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot>
- Вештачка интелигенција у сигурносним системима, <https://vectra.ai/learning/ai-security2>

Преглед

- 1 Увод: о сајбер криминалу
- 2 Мере заштите
- 3 Закључак

Увод: о сајбер криминалу

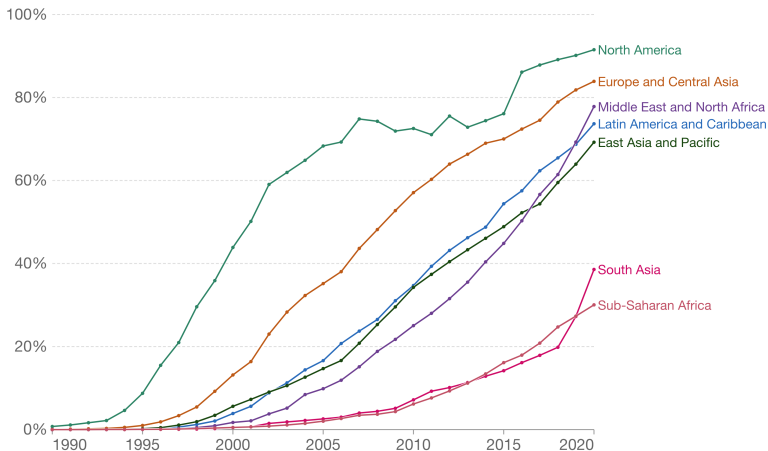
- Мотиви за сајбер криминал:
 - крађа и продаја података,
 - шпијунажа,
 - бесплатно коришћење програма и мултимедијалних садржаја
- Стање сајбер криминала:
 - већина великих организација је претрпела сајбер нападе
 - IDS (Intrusion Detection System) системи нису решили проблеме
 - велики број умрежених рачунара за дистрибуцију пиратерије
 - сајбер криминал је статистички најдоминантнији тип криминала

Пораст коришћења интернета у свету током година

Share of the population using the internet

Share of individuals who have used the Internet from any location in the last 3 months.

Our World
in Data



Source: International Telecommunication Union (via World Bank)

OurWorldInData.org/technology-adoption/ • CC BY

Note: Internet usage includes computers, mobile phones, personal digital assistants, games machines, digital TVs, etc.



Мере заштите

- Мере заштите које могу применити појединци
 - опрезност на интернету
 - редовно ажурирање оперативног система и антивирусног софтвера
 - коришћење комплексних лозинки
 - креирање резервних копија података
- Додатне мере заштите које могу примењивати организације
 - спровођење редовних обука из домена сајбер безбедности
 - креирање профила за приступ
 - креирање процедура за поступање у случајевима напада
 - употреба анализе рањивости
 - коришћењем мамаца ханипотова

Шта даље очекивати

- Све већи број сајбер напада и њиховог утицаја на нас
- Развој AI сигурносних система
- Коришћење AI у развијању малициозних програма