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`

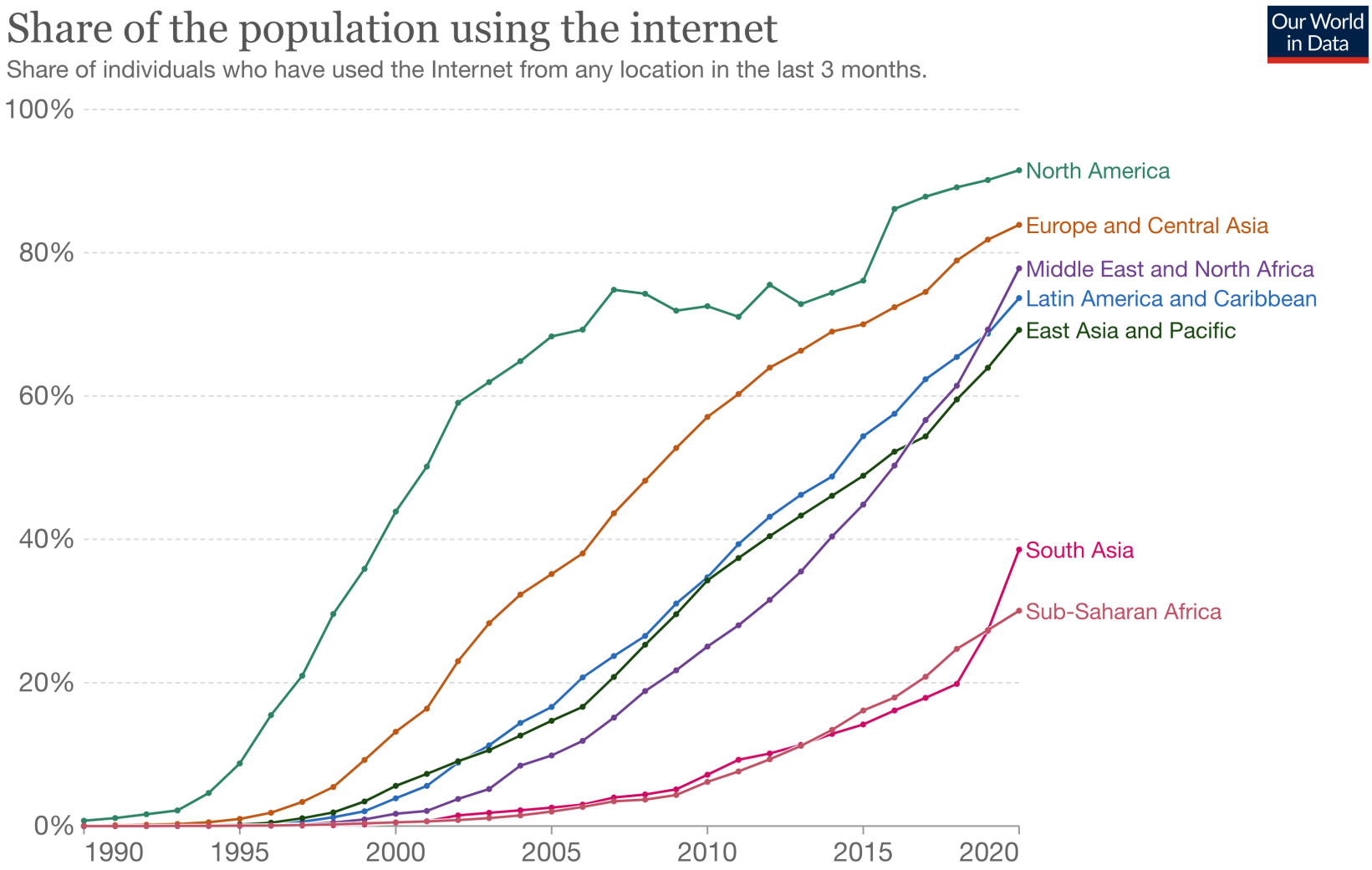
Преглед

1. Сајбер криминал
   - Типови сајбер криминала
   - Примена у пракси
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 (Intrustion Dectection 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



Типови сајбер криминала

- Типови сајбер криминала:
  - Сајбер криминал у ужем смислу
  - Сајбер криминал у ширем смислу
- Конкретни облици сајбер криминала:
  - Неовлашћен приступ
  - Оштећење података или програма
  - Неовлашћено пресретање комуникација
  - Саботажа
  - Шпијунажа
- Учиниоци дела сајбер криминала:
  - Злонамерни учиниоци
  - Учиниоци не мотивисани проузроковањем штете

Примена у пракси

- Владимир Левин, софтверски инжењер из Петрограда, краде 10 милиона долара из Citybank-a
- „Црв" Морис 1998. године
- Џонатан Џозеф Џејмс упада у Агенцију Министарства Одбране и НАСУ 1999.
- 2003. године црв наноси штету од 1.2 милијарде долара
- Украјинска криминална организација фалсификује кредитне картице 2009.
- Случај AshleyMadison.com
- Авионски инцидент 2015. године

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 применити организације
  - спровођење редовних обука
  - 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