Informačné vzdelávanie

**Bezpečnosť - šifrovanie**

**Meno autora** : Emma Macháčová

**Dátum vytvorenia** : 15.11.2019

**Obsah**

[Abstrakt 1](#_Toc24635313)

[1. Úvod 2](#_Toc24635314)

[2. Počítačová bezpečnosť 3](#_Toc24635315)

[3. Ako zabezpečiť počítačovú bezpečnosť 4](#_Toc24635316)

[**3.1. Hrozby pre počítačovú bezpečnosť** 4](#_Toc24635317)

[**3.2. Bezpečnostné aplikácie a opatrenia** 4](#_Toc24635318)

[4. Šifrovanie 5](#_Toc24635319)

[**4.1. Princíp šifrovania** 5](#_Toc24635320)

[**4.1.1. Šifrovacie kľúče** 5](#_Toc24635321)

[**4.1.2. Typy šifrovacích kľúčov** 5](#_Toc24635322)

[**4.2 Druhy šifrovania** 5](#_Toc24635323)

[5. Dešifrovanie 6](#_Toc24635324)

[**5.1. Princíp dešifrovania** 6](#_Toc24635325)

[5. Záver 7](#_Toc24635326)

[6. Zoznam použitej literatúry 8](#_Toc24635327)

[7. Zoznam obrázkov 9](#_Toc24635328)

# **Abstrakt**

# **1. Úvod**

- co za pracu pisem, preco ju pisem, o com ju pisem..

# **2. Počítačová bezpečnosť**

## **2.1. Čo je to počítačová bezpečnosť**

Vo väčšine literatúry sa počítačová, alebo kybernetická bezpečnosť používa ako všeobecný pojem. Napríklad slovník Merriam Webster ho definuje ako „opatrenia prijaté na ochranu počítača alebo počítačového systému (na internete) pred neoprávneným prístupom alebo útokom“. Medzinárodná telekomunikačná únia (ITU) zase definuje kybernetickú bezpečnosť takto :

„Kybernetická bezpečnosť je súbor nástrojov, politík, bezpečnostných konceptov, bezpečnostných záruk, usmernení, prístupov k riadeniu rizika, akcií, školení, osvedčených postupov, uistenia a technológií, ktoré možno použiť na ochranu počítačového prostredia a majetku organizácie a používateľa. Medzi aktíva organizácie a používateľa patria pripojené počítačové zariadenia, personál, infraštruktúra, aplikácie, služby, telekomunikačné systémy a celkový počet prenášaných a / alebo uložených informácií v kybernetickom prostredí. Cybersecurity sa snaží zabezpečiť dosiahnutie a udržiavanie bezpečnostných vlastností organizácie a majetku používateľa proti relevantným bezpečnostným rizikám v kybernetickom prostredí.“

Whitman a Mattord (2009) definujú bezpečnosť informácií ako „ochranu informácií a jej kritických prvkov vrátane systémov a hardvéru, ktoré tieto informácie používajú, ukladajú a prenášajú“ (Whitman a Mattord, 2009, s. 8). Títo autori tiež identifikujú niekoľko kritických charakteristík informácií, ktoré jej dávajú hodnotu v organizáciách. Medzi tieto vlastnosti patrí dôvernosť, integrita a dostupnosť informácií, ako sa uvádza v definícii uvedenej v ISO / IEC 27002 (2005), ale neobmedzujú sa iba na tieto tri charakteristiky.

### **2.1.1 Existuje rozdiel medzi informačnou bezpečnosťou a kyber-bezpečnosťou?**

vlastný názor

## **2.2. Všeobecné bezpečnostné ciele**

Cieľom informačnej bezpečnosti je zabezpečiť kontinuitu podnikania a minimalizovať obchodné škody obmedzením dopadu bezpečnostných incidentov (Von Solms, 1998).

Medzi hlavné bezpečnostné ciele patrí :

1. Dostupnosť
2. Integrita, ktorá môže zahŕňať autentickosť a nevypovedanie
3. Dôvernosť ITU, 2008.

<https://www.sciencedirect.com/science/article/pii/S0167404813000801>

- na co to je dobre?

- na co sluzi, vyznam?

- "cyber security" OR "internet safety"

- https://www.sciencedirect.com/science/article/pii/S0167404813000801

- Cyber-Security, Computer security, Risk, Threat, Vulnerability

- "security" AND "encryption"

- https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.95.4226

- "security" AND "data encryption"

- https://dl.acm.org/citation.cfm?id=358718

- Cryptography, Data management systems, Data layout

# **3. Ako zabezpečiť počítačovú bezpečnosť**

## **3.1. Hrozby pre počítačovú bezpečnosť**

- proti akym hrozbam treba bojovat?

- aké bezpečnostné hrozby existujú?

- "computer security" AND "threat"

- <https://patents.google.com/patent/US8239668B1/en>

## **3.2. Bezpečnostné aplikácie a opatrenia**

- ake bezpecnostne aplikacie existuju?

- ake opatrenia su mozne na lepsie zabezpecenie?

- co su to certifikaty, ako sluzia, kto ich poskytuje?

- "cyber security" AND "tools"

- <https://www.sciencedirect.com/science/article/pii/S0167404810000775>

- Information security enforcement

- "cyber security applications"

- <https://link.springer.com/chapter/10.1007/978-3-319-16549-3_5>

- Intrusion Detection

# **4. Šifrovanie**

- co to znamena v ramci informacnych technologii?

- ake je vyuzitie sifrovania?

## **4.1. Princíp šifrovania**

- ako to funguje?

### **4.1.1. Šifrovacie kľúče**

- popis, princip prace :

- ako su v sifrovani vyuzivane sifrovacie kluce?

- ako funguju sifrovacie kluce? ako vznikaju?

- ako ich (sif. kluce) realne vyuzivaju uzivatenia?

### **4.1.2. Typy šifrovacích kľúčov**

- typy sifrovacich klucov (public key..)

- "encryption key"

- https://patents.google.com/patent/US9002018B2/en

- "key encryption"

- https://link.springer.com/chapter/10.1007/3-540-39200-9\_16

- Bilinear Diffie-Hellman, Forward security, Key exposure

## **4.2 Druhy šifrovania**

- ake su druhy sifrovania?

- aky je rozdiel medzi symetrickym a asymetrickym sifrovanim?

# **5. Dešifrovanie**

- co to je?

## **5.1. Princíp dešifrovania**

- ako funguje?

- ako sa to lisi od sifrovania?

- co je to cyberspace?

- SSL/TLS?

- cloud copmuting - co to je, na co to sluzi:

- "security" AND "data encryption"

- https://patents.google.com/patent/US5999629A/en

# **5. Záver**

# **6. Zoznam použitej literatúry**

# **7. Zoznam obrázkov**