TECHNICKÉ ZABEZPEČENIA

Boris Ch. Mavrodiev VI.OA

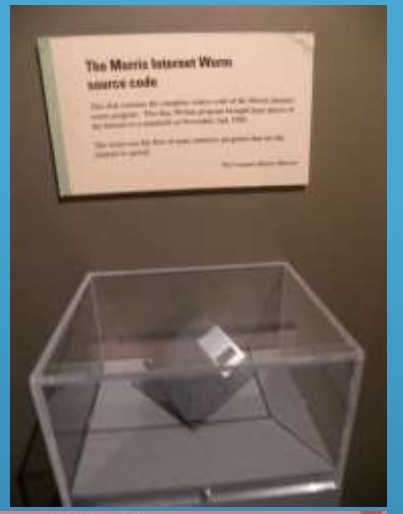
ZABEZPEČENIE POČÍTAČA

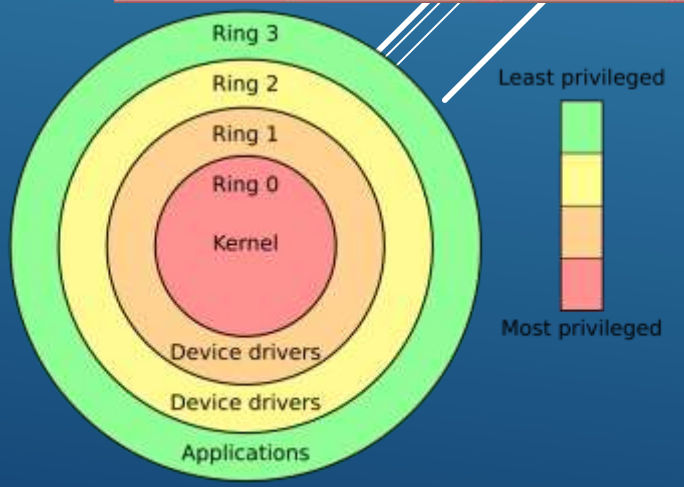
OS A APLIKÁCIE

- Používanie legálneho softvéru
  - Legálne OS a aplikácie sú pravidelne aktualizované a „zaplátané“, čo znižuje bezpečnostné riziká
  - Garancia „kódovej čistoty“ – neobsahuje neautorizované úpravy
- Udržovanie OS a aplikácií aktualizovanými
  - Aktualizácie opravujú bezpečnostné diery
- Používanie antivírusového programu
  - Používanie viacerých naraz nie je odporúčané – rušia sa

MALWARE (ŠKODLIVÝ SOFTVÉR)

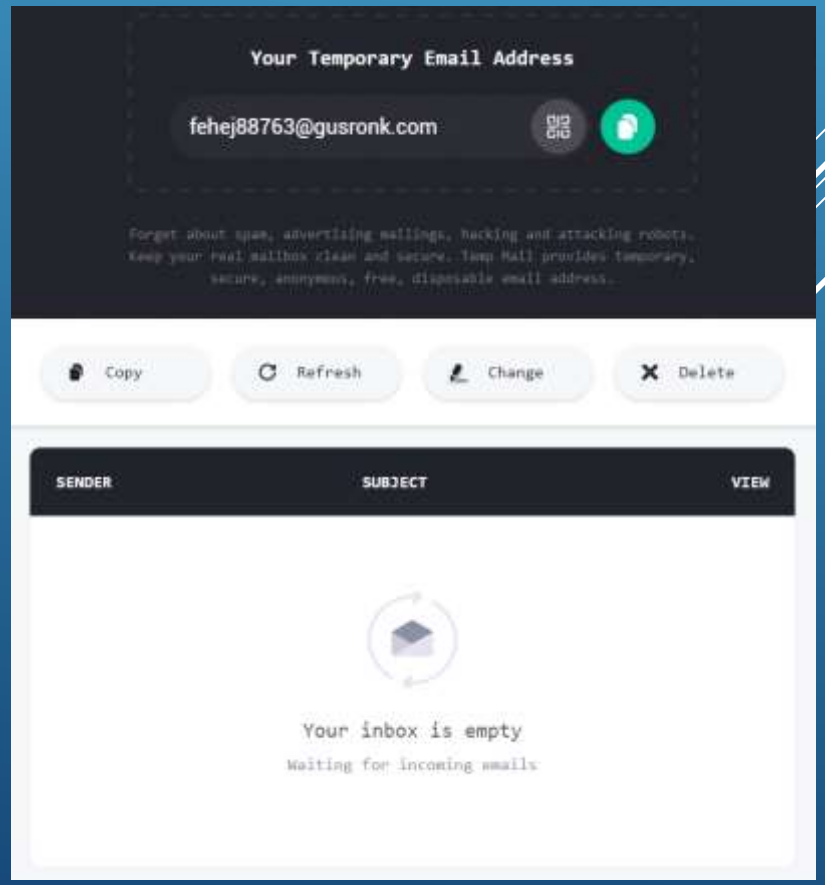
- **Červ** (Worm) – po napadnutí počítača sa kopíruje a šíri ďalej
  - Prvý - Morrisov červ (**The Morris Worm**) - ARPANET
- **Trojský kôň** (Trojan) – navonok pôsobí ako užitočný program, ale umožňuje útočníkovi preniknúť cez „zadné vrátka“ (backdoor)
  - Najčastejší – RAT (Remote Access Trojan)
- **Spyware** – sleduje aktivitu užívateľa
- **Adware** – vystavuje užívateľa neželaným reklamám
- **Ransomware** – zašifruje dáta v počítači špecifickým kľúčom a žiada výkupné
  - Najznámejší, najagresívnejší a najničivejší – **WannaCry** (12.5.2017)
- **Rootkit** – skrýva sa v jadre (kerneli) OS (väčšinou Ring 0 alebo Ring 1)
  - Ťažko sa identifikuje a odstraňuje
  - Umožňuje útočníkovi trvalý a často neviditeľný prístup k celému systému a dátam





BEZPEČNOSŤ NA INTERNETE

- Firewall - riadi dátový tok medzi počítačom a internetom
- Používať svoj osobný email iba na dôveryhodné veci
  - Používať „disposable email“ (alebo alternatívny email) a nie svoje heslá na jednorazové veci na internete
    - Príklad jednorazovej adresy – nesepoc512@gusronk.com, fehej88763@gusronk.com (https://temp-mail.org)
    - Príklady alternatívnej adresy – anazjarkumaradarozky@gmail.com, oprazenacibulka@seznam.cz
    - Príklady primitívneho hesla – qWertY123456, nbusk123, gjar0000
- Vyhýbať sa komunikácii s neznámymi ľuďmi mimo kontextu situácie
  - „Online spoluhráči nech ostanú online spoluhráčmi“
  - Nič o sebe neprezrádzať neznámym ľuďom na internete
- Používať šifrované komunikačné aplikácie a protokoly
- **Heslový manažment**



BEZPEČNOSŤ NA SOCIÁLNYCH SIEŤACH

- **OSINT** – **O**pen **S**ource **Int**elligence
  - Spravodajstvo z otvorených zdrojov
  - Národná bezpečnosť, právne orgány, žurnalisti, ale aj civilisti (či už s dobrými alebo zlými úmyslami)
  - Internetový vyhľadávač, sociálne siete a fóra, dark web, ...
- **Digital footprint** (Digitálna stopa) – súbor údajov o online aktivitách jednotlivca
  - História, príspevky, komentáre, nákupy, ...
- **Heslový manažment**

HESLOVÝ MANAŽMENT

- Silné heslá na vami zvážené najkritickejšie oblasti (napr. bankovníctvo, sociálne siete, mailová schránka, účty od úložísk)
  - Aspoň 9 znakov, malé aj veľké písmená, čísla a špeciálne znaky) – napr. PhLjt4&AwjO
- Jedinečné heslo na každú službu
- Pravidelná aktualizácia hesiel a kontrola únikov (https://haveibeenpwned.com)
- Dvojfaktorové overovanie (2FA)
  - osobné odporúčanie – Authentification aplikácie (napr. Google Authentificator, Authy)

```c
#include <stdio.h>
#include <stdlib.h>
#include <time.h>

int main(void) {
    srand((unsigned) time(NULL));
    int pocet, starsie;
    printf("Zadaj pocet znakov: ");
    scanf("%d", &pocet);
    printf("Bude heslo pouzivane v starsich heslovych systemoch [0 pre nie / 1 pre ano]: ");
    scanf("%d", &starsie);

    char znaky[] = {'!', '\"', '#', '$', '%', '&', '\'', '(', ')', '*', '+', ',', '-', '.', '/', ':', ';', '<', '=', '>', '?', '@', '[', '\\', ']', '^', '_', '`'};
    char znaky_starsie[] = {'!', '#', '$', '%', '&', '(', ')', '*', '+', '-', '.', '/', ';', '=', '@', '[', ']', '^', '_', '`'};

    char *heslo = malloc(pocet + 1);
    if (!heslo) {
        printf("Nepodarilo sa alokovat pamat.\n");
        return 1;
    }

    for(int i = 0; i < pocet; i++) {
        char c;
        switch(rand() % 4) {
            case 0:
                c = 'A' + (rand() % 26);
                break;
            case 1:
                c = 'a' + (rand() % 26);
                break;
            case 2:
                c = '0' + (rand() % 10);
                break;
            case 3:
                if(starsie){
                    int dlzka = sizeof(znaky_starsie) / sizeof(znaky_starsie[0]);
                    c = znaky_starsie[rand() % dlzka];
                }
                else {
                    int dlzka = sizeof(znaky) / sizeof(znaky[0]);
                    c = znaky[rand() % dlzka];
                }
                break;
        }

        heslo[i] = c;
    }

    heslo[pocet] = '\0';

    printf("Vygenerovane heslo je: %s", heslo);

    free(heslo);
    return 0;
}
```

MOJE RADY

- Nespoliehať sa **len** na AV
  - Byť na internete skeptický, opatrný, „paranoidný“ a používať zdravý rozum
- Rozumieť OS, ktorý používate a vedieť, čo a ako funguje
- Nesťahovať spustiteľné súbory a skripty (*.exe, *.cmd, *.bat) z neznámych a nedôveryhodných zdrojov (najmä prílohy nevyžiadaných emailov alebo emailov z neznámej adresy)

ZABEZPEČENIE DOMÁCEJ POČÍTAČOVEJ SIETE

- Zmena predvoleného (továrenského) hesla administrácie routeru
- Pravidelná aktualizácia firmvéru (ovládací softvér) routeru
  - Oprava zraniteľností
- Zabezpečenie siete heslom a šifrovaním
  - Minimálne WPA2-PSK
- Filtrovanie nežiadúcich pripojení do siete prostredníctvom MAC adresy
- Aktívny firewall routeru

ZDROJE

- https://e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1653-jak-zabezpecit-pocitac
- https://e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1651-jak-zabezpecit-domaci-pocitacovou-sit
- https://www.ibm.com/think/topics/osint
- https://appcheck-ng.com/what-is-open-source-intelligence-osint
- https://haveibeenpwned.com/
- https://temp-mail.org/

ĎAKUJEM ZA POZORNOSŤ