Bezpečnostní manuál OPEN DOORS ver. 04/15_3

Zabezpečení PC (platforma Windows) - členové OPEN DOORS

Pro zabezpečení osobního počítače, laptopu atd. uvažujeme platformu s OS Windows:

1. **Antivirus** - používat jakýkoliv aktualizovaný antivirus. Nedoporučuje se používat neaktualizovaný jako např. MS Essentials . Pro základní zabezpečení doporučen free antiviru AVAST, ke stažení Základní verze https://www.avast.com/cs-cz/index . Na PC provozovat POUZE jeden jediný antivirus
2. **Kontrola a odstraňování spyware**
   a. Aplikace Malwarebytes free version http://www.malwarebytes.org/antimalware/
   b. SuperANTISpyware free edition http://www.superantispyware.com/downloadfile.html?productid=SUPERANTISPYWAREFREE
   c. Spybot home user Free edition http://www.safer-networking.org/private/

Všechny aplikace je doporučeno nainstalovat a udržovat aktualizované. Aplikace ze sekce „Kontrola a odstraňování spyware“ je nutno po nainstalování nastavit tak, aby **nepracovaly** v pozadí. Aplikace ze sekce „Kontrola a odstraňování spyware“ je doporučeno **spouštět postupně 1 x za 14 dnů** a nechat jimi zkontrolovat celý počítač (všechny lokální disky popř. připojená média např. typu USB disk či SD karta).

Zabezpečení zařízení s OS Android - členové OPEN DOORS

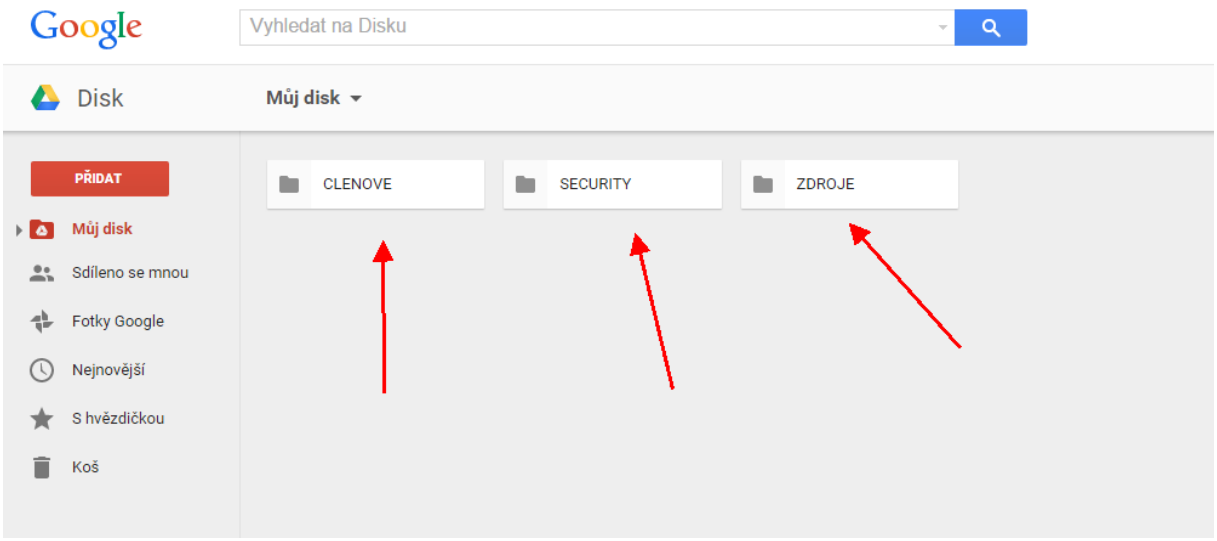
Pro zabezpečení osobního počítače, laptopu, smartphone atd. uvažujeme platformu s OS Android:

1. Antivirus - používat antivirus, který je šetrný k paměti zařízení. Doporučen Zoner Antivirus, buď ve free či placené verzi viz https://play.google.com/store/apps/details?id=com.zoner.android.antivirus
2. Kontrola a odstraňování spyware - antivirem Zoner Antivirus nechat 1 x týdně projet celé zařízení. V případě napadení jakékoliv aplikace, je nutné tuto aplikaci nechat odinstalovat. Následně je možné odinstalovanou apliakci znovu naisntalovat přes Google play Store a znovu nechat projet celé zařízení antivirem Zoner Antivirus.

Přístup na sdílené úložiště Google DISK OPEN DOORS

Na adrese https://drive.google.com je k dispozici úložiště iniciativy, kam někteří členové mohou nahrávat a sdílet potřebný materiál. Přístupové jméno je **cz.opendoors@gmail.com**, heslo bylo zasláno členům (ti kteří pracují se zdroji) via SMS.

Základní struktura Google DISKU



A. Složka CLENOVE slouží pro jednotlivé členy iniciativy a v ní jsou vnořeny podsložky s jejich příslušným označením (jménem)
B. Složka SECURITY slouží k uchovávání informací o bezpečnostních opatřeních v rámci iniciativy
C. Složka ZDROJE a její podsložky je vyhrazena pro uchovávání informací od zdrojových osob, organizací atd.
D. Další složky mohou postupně přibývat

V případě, že člen OPEN DOORS ztratí přístupové údaje k DISKU Google či mu je přístup odcizen třetí stranou, člen je povinen okamžitě vyrozumět admina DISKU (Radim na telefonním čísle +420724112498). Admin provede změnu uživatelského hesla.

Vzhledem k tomu, že jednotlivé soubory a složky jsou sdílené pod jedním účtem, všichni členové OPEN DOORS musí dávat pozor, aby nedocházelo k dublování verzí či struktury. V případě editování dokumentu by měl editaci provádět pouze jeden člen ve stejný čas.

Internetové přístupy členů OPEN DOORS

V kavárnách a jiných veřejných prostorách, kde je k dispozici Wi-Fi hotspot zásadně nepoužívat připojení k tomuto zdroji Internetu! Pro připojení používat separátní internetové připojení například přes vlastní mobilní telefon. Wi-Fi připojení používat jen v domácím prostředí nebo

v ověřených (neveřejných) prostorách.

Chování člena OPEN DOORS na facebooku / twitteru (Internetu)

Členům OPEN DOORS je VELMI doporučeno si přečíst následující články věnující se bezpečnosti na Internetu:

http://cs.wikipedia.org/wiki/Bezpe%C4%8Dnost_na_internetu

http://www.bezpecnyinternet.cz/zacatecnik/on-line-komunikace/rizika.aspx

http://www.lupa.cz/clanky/instant-messaging-nepravem-prehlizena-hrozba/

http://euro.e15.cz/archiv/ocima-kremelskeho-trolla-rusko-zamestnava-armadu-internetovych-diskuteru-1180090

Na Internetových sociálních sítích (popř. emailu) dále **NENÍ doporučeno**:

- Klikat na odkazy, o kterých nejsem 100% přesvědčen, že jsou bezpečné. V opačném případě riskuji zavlečení spyware na mé zařízení a ohrožení nejen sebe, ale i přátel (řetězová reakce)
- Hrát online hry (jsou semeništěm různého malwaru/spyware). Opět tím ohrožuji nejen sebe.

Na Internetových sociálních sítích (popř. emailu) dále **JE VELMI doporučeno**:

- 1x za měsíc změnit heslo k účtu

Interní chat - Instant Messaging (internal IM)

IM je důležitým faktorem při dorozumívání členů OPEN DOORS. Vzhledem k tomu, že OPEN DOORS facebook chat (PM) je velmi lehce napadnutelný a bez možnosti enkrypce datového provozu, iniciativa OPEN DOORS se rozhodla, že s platností od 27. 04. 2015 se bude používat jako jediné IM médium pro interní online IM služba Bleep jak pro platformu Windows, tak pro Android:

Instalace ke stažení: http://labs.bittorrent.com/bleep/

Po nainstalování je nutno zadat přihlašovací jméno, emailovou adresu a nechat si na mail poslat aktivační kód.