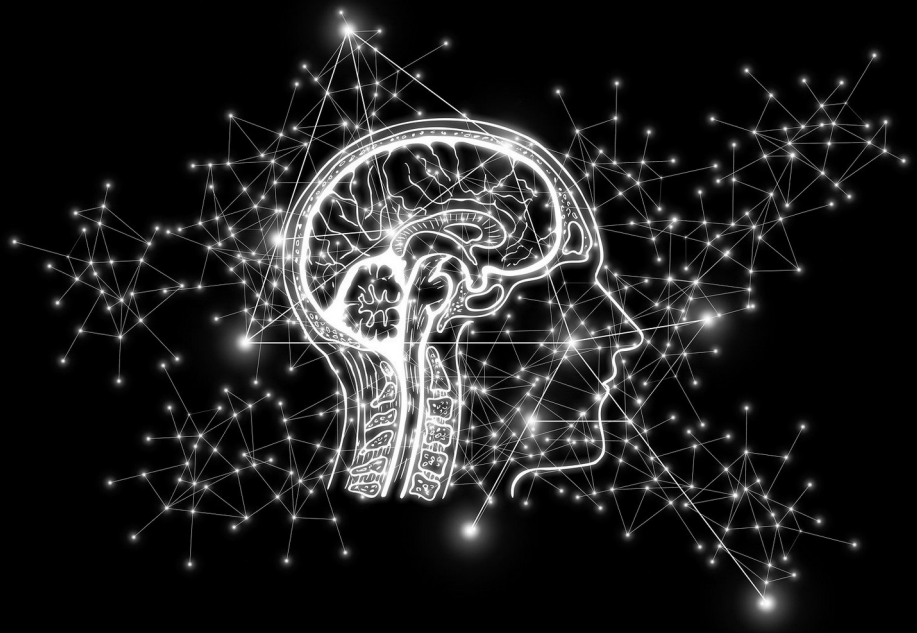


Riziká a nástrahy virtuálneho priestoru

Peter Šantavý

Úvod

Prečo školenie?

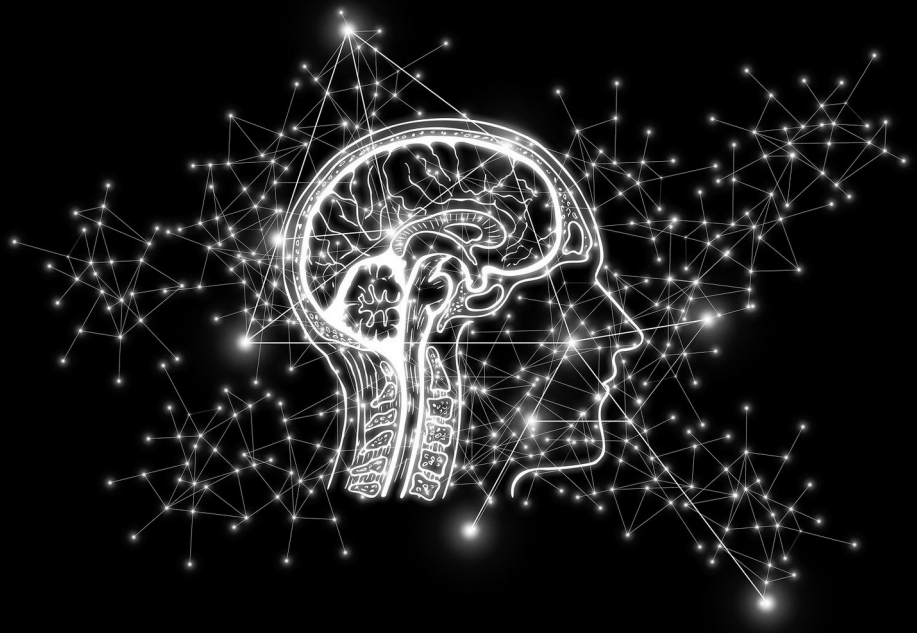
Človek je najslabší článok kybernetickej bezpečnosti

- väčšina útokov je spôsobená **ľudskou chybou**
- dlhodobo je **kybernetická kriminalita na vzostupe**
- **sme viazaní legislatívou** a dodržiavaním pravidiel
- máme **zodpovednosť** voči tým, ktorí nám svoje údaje zverujú

Na čo treba pamätať!

- informačná a kybernetická **bezpečnosť je proces**,
  nie jednorazový úkon
- potrebné je **vytvoriť si bezpečnostné návyky**,
  nielen o bezpečnosti počuť alebo poznať pravidlá

Človek je najslabší článok kybernetickej bezpečnosti!



Riziká a nástrahy virtuálneho priestoru

Peter Šantavý

Kybernetická bezpečnosť

Škodlivý kód (malvér/malware)

Škodlivý kód, ktorý infikuje nielen počítač, ale i celé siete

- rôzne **druhy**: ransomware, spyware, cryptominer, trojan, worm,...
- rôzne **ciele**: plošné/cielené, o čo útočníkom ide...
- rôzne **spôsoby šírenia**: e-mail, web, usb, QR kód, sociálne siete,...
- rôzne **zariadenia v sieti**: mobily, tablety, súkromné zariadenia

Potrebné je vytvoriť si bezpečnostné návyky, nielen o bezpečnosti počuť!

Bezpečnostné školenie I.

1. Ako sa vyhnúť malvéru?

čo to je malvér;

aké typy škodlivého kódu existujú,

čo sú jeho ciele, ako sa šíri

a aké hrozby striehnu na mobilné zariadenia.

Odkaz na školenie o malvéri...

Na školenie o malvéri odkazuje zobrazený QR kód...

Bezpečné používanie internetu

Internet môže skrývať rôzne nebezpečenstvá

- **verejná** WiFi: únos spojenia, VPN, WiFi vs. mobilné dáta,...
- práca na diaľku (**home office**): rizikové domáce siete/zariadenia, zdieľanie,...
- **bezpečné** prehliadanie: riziká na stránkach, prehliadače a ochrana,...
- **filtrovanie** obsahu: detský zámok, rizikové stránky a obsah,...
- bezpečné **vyhľadávanie**: reklamy, odkazy, obsah na neznámych stránkach,...

Kybernetická bezpečnosť je proces, nie jednorazový úkon!

Bezpečnostné školenie II.

2. Bezpečné používanie internetu

bezpečné používanie verejných Wi-Fi sietí;

práca na diaľku;

bezpečné prehliadanie webu;

filtrovanie nežiadúceho obsahu;

práca s vyhľadávačom.

Odkaz na školenie o internete...

Na školenie o bezpečnosti na internete odkazuje zobrazený QR kód...

Ochrana bezpečnými heslami

Ochrana prístupu k digitálnym účtom a aktívam

- **silné heslá**: ako ich vytvoriť?
  jedinečnosť, dĺžka, fráza vs. info o mne, špeciálne znaky, slovníkové heslá,...
- **zaobchádzanie** s heslami: správca hesiel (password manager)
  unikátne heslá, zmena hesla, kde ich ukladať?
- **zvýšenie bezpečnosti**: MFA/2FA, passwordless overenie
  viacfaktorová autentifikácia ako poistka k heslu, resp. nahradenie hesla pre bezpečný prístup

Potrebné je vytvoriť si bezpečnostné návyky, nielen o bezpečnosti počuť!

Bezpečnostné školenie III.

3. Ochrana bezpečnými heslami

heslo ako prostriedok pre zabezpečenie digitálnych účtov; vytvorenie silného hesla; zaobchádzanie s heslami; používanie ďalšej formy overenia.

Odkaz na školenie o heslách...

Na školenie o bezpečných heslách odkazuje zobrazený QR kód...

Bezpečie e-mailovej komunikácie

(nielen) E-mail – klasický komunikačný nástroj i vstupná brána útoku

- **vektor útoku**: zneužitie chyby systému, oklamanie používateľa,...
  vylákanie citlivých informácií, vykonanie nesprávnej operácie, infiltrácia malvéru,...
- **phishing** – kybernetický podvod: spearphishing, znaky phishingu
  generické oslovenie, neočakávaný email, časový nátlak, lákavá ponuka,...
- **prílohy** e-mailov: infiltrácia malvéru, spolupráca pri aktivácii, rozpoznanie
- **spam –** nevyžiadaná komunikácia: neotvárať, neklikať, nepreposieľať

Kybernetická bezpečnosť je proces, nie jednorazový úkon!

Bezpečnostné školenie IV.

4. Bezpečie e-mailovej komunikácie

e-mail ako vektor útoku;

ako vyzerá phishing;

podozrivé prílohy;

spam.

Odkaz na školenie o e-mailoch...

Na školenie o zabezpečení e-mailov odkazuje zobrazený QR kód...

Ochrana pred cielenými hrozbami

Cielené útoky a manipulácia šitá na mieru; skryté domáce hrozby

- **sociálne inžinierstvo**: psychologické a manipulačné techniky

  získanie dôverných informácií, prístup k citlivým systémom, procesné zlyhania,...

- **vnútorné hrozby**: ľudia, informačné systémy, procesy

  neznalosť a neúmyselné zlyhanie, zámerné škodlivé konanie, nechránené systémy,...

Potrebné je vytvoriť si bezpečnostné návyky, nielen o bezpečnosti počuť!

Bezpečnostné školenie V.

5. Ochrana pred cielenými hrozbami

cielené útoky; manipulácia šitá na mieru;

praktiky sociálneho inžinierstva;

hrozby číhajúce zvnútra firmy.

Odkaz na školenie o cielených hrozbách...

Na školenie o cielených hrozbách odkazuje zobrazený QR kód...

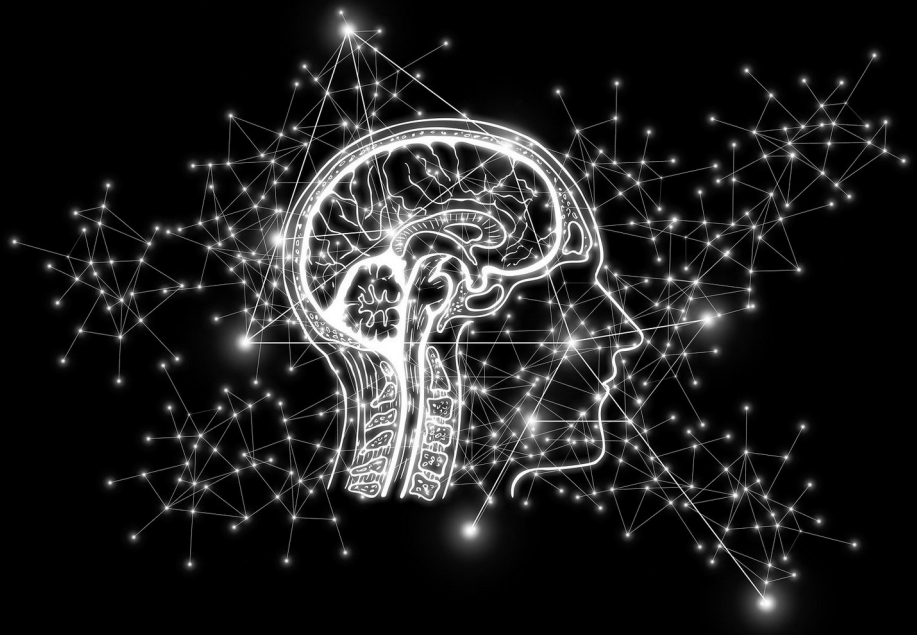
Bezpečnostné školenie VI.

Bezpečnostné riziká na cestách a mimo bežného pracovného prostredia

- využívanie verejných USB nabíjačiek
- verejné wifi – bezdrôtové pripojenie na námestiach, v hoteloch, reštauráciách a pod.
- využívanie cudzej techniky
- využívanie QR kódov
- zopakovanie základných pravidiel informačnej bezpečnosti
- **informovanie o informačných incidentoch**

Odkaz na bezpečnostné riziká na cestách...

Na informácie o hrozbách na cestách odkazuje zobrazený QR kód...



Riziká a nástrahy virtuálneho priestoru

Peter Šantavý

Niektoré problémy v organizáciách

Oddelenie dát a cloudové služby

Problém – počítače s nastavenými cloudovými účtami

- **Microsoft 365, Google, Apple iCloud,...**

  Dáta organizácie sa v počítači nesmú miešať s dátami osobných/iných pracovných účtov!!!

- **externé cloudové služby, „šedá zóna“ IT**

  Osobné údaje a interné dáta organizácie sa nesmú ukladať, resp. zdieľať na externých cloudových službách, ktoré nemáme pod kontrolou...

  Riziká „šedej zóny“: únik údajov a vektor útoku na organizáciu...

Aké môžu byť výnimky pre využívanie externých služieb?

Posielanie a zdieľanie dát

Problém – narábanie s veľkými súbormi (príklad ABÚ)

- **Groupwise (prenos dát v prílohách emailov)**

  – miesto veľkých príloh posielať odkazy na vyzdieľanie súborov cez Filr.

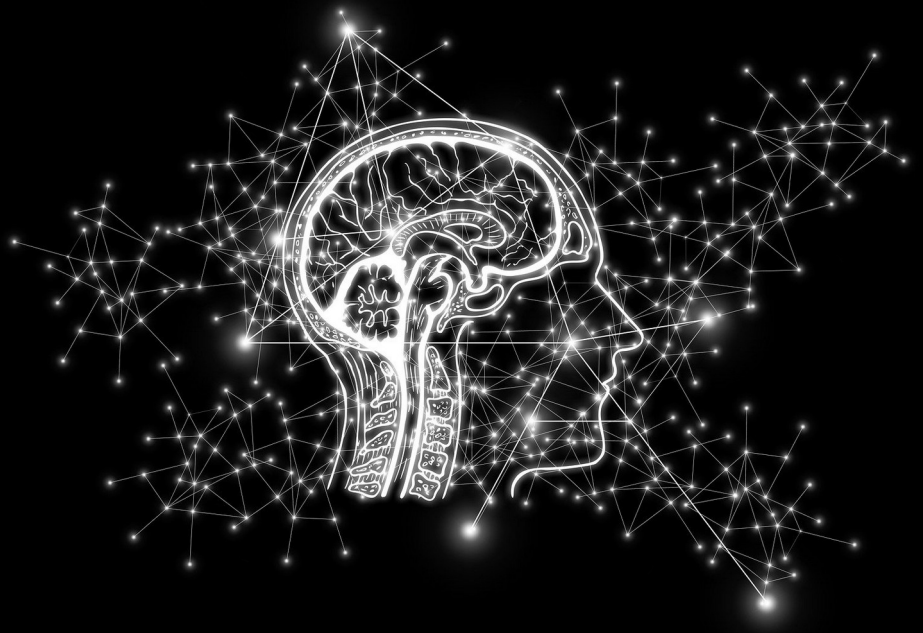
- **Zdieľané úložisko dokumentov Filr**

  – možnosť zdieľať dáta s internými i externými používateľmi

  – pokročilé možnosti zdieľania súborov (časovo obmedzené, zabalené s heslom,...)

- **Prenosné médiá:** USB, CD/DVD,...

Nastavené a dodržiavané pravidlá narábania s údajmi mimo organizácie (nosiče, počítače,...)



Ďakujem za pozornosť

ThLic. Ing. Peter Šantavý, PhD.
peter.santavy@uniba.sk