MUNI
ICS

Kyberbezpečnost

Tomáš Plesník et al.

CSIRT-MU, 24. 11. 2021

Co nás čeká?

Kyberhygiena

- 1. přednáška – 24. 11. 2021
- *„Těžko na cvičišti…“*
- **Jak se bránit**

Kybernetické útoky

- 2. přednáška – 1. 12. 2021
- *„Lehko na bojišti!“*
- **Čemu se bránit**

Představení

Tomáš Plesník (přednášející)

- Vedoucí Bezpečnostního týmu – CSIRT-MU
- Manažer KB MUNI dle z. č.181/2014 Sb.
- Správce zabezpečeného IS dle z. č. 412/2005 Sb.
- Řešitel (mezi)národních projektů v oblasti KB
- https://www.muni.cz/lide/207426-tomas-plesnik

MUNI ICS

Představení

Miriam Gáliková

- Členka Bezpečnostního týmu – CSIRT-MU
- Specialistka kybernetické bezpečnosti
- Specialistka na osvětu a vzdělávání v oblasti KB
- Lektorka školení uživatelů a U3V
- https://www.muni.cz/lide/500327-miriam-galikova

MUNI ICS

Představení

Petra Mikulová

- Člen Bezpečnostního týmu – CSIRT-MU
- Specialistka na osvětu a vzdělávání v oblasti KB
- Lektorka školení uživatelů a U3V
- Konzultantka orgranizace Iuridicum Remedium
- Spoluautorka osvětových kurzů Kybernetické bezpečnosti
- https://www.muni.cz/lide/243499-petra-mikulova

MUNI ICS

Disclaimer

Cyber Security

⇔*

Kybernetická bezpečnost

⇔*

Kyberbezpečnost

(* alespoň v rámci této přednášky)

Definice

Kybernetická bezpečnost

„Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.“

Zdroj: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

Regulace

Kybernetická bezpečnost

- **Zákon č. 181/2014 Sb. *Zákon o kybernetické bezpečnosti (ZoKB)***
  - Implementace směrnice Evropského parlamentu a Rady EU (NIS Directive)
  - Aktuálně v přípravě nová verze směrnice (NIS 2 Directive) – očekávaná implementace v 2024
- **Vyhláška č. 82/2018 Sb. *Vyhláška o kybernetické bezpečnosti (VoKB)***
  - Na základě normy ISO/IEC 27000 (ISMS) – zavedení SŘBI v organizaci
- Regulace z pohledu národní autority – NÚKIB
  - Systémy KII, ISZS a VIS
  - **Na MUNI celkem 2 VIS – IS MU a ESIS MU**

Motivace

Kybernetická bezpečnost

- Rychle rostoucí míra **digitalizace společnosti** a její **silná závislost** na IS/ICT
- **Stírající se hranice** mezi on-line a off-line světem
- **Kyberhygiena** a **orientace v kyberprostoru** základem všeobecného přehledu člověka 21. století
- **Elektronizace všemožných agend** (nejen státní správy)
- **Pandemie a s ní související trendy** – home-office a distanční formy výuky

- Potřeba **zvyšování digitální gramotnosti** populace
- **Problém celé společnosti** – nejen asociálních, dlouhovlasých a nemytých „Ajťáků“

MUNI
ICS

Kyberhygiena

Co je Kyberhygiena a proč je důležitá?

- Pomocí kyberhygieny **udržujeme svá data a zařízení v dobrém stavu** a zvyšujeme svou bezpečnost
- **Tvořena většinou z drobností**, které dokáží ochránit nás a naše data
- Dodržování těchto zásad navíc **není až zas tak složité**

MUNI ICS

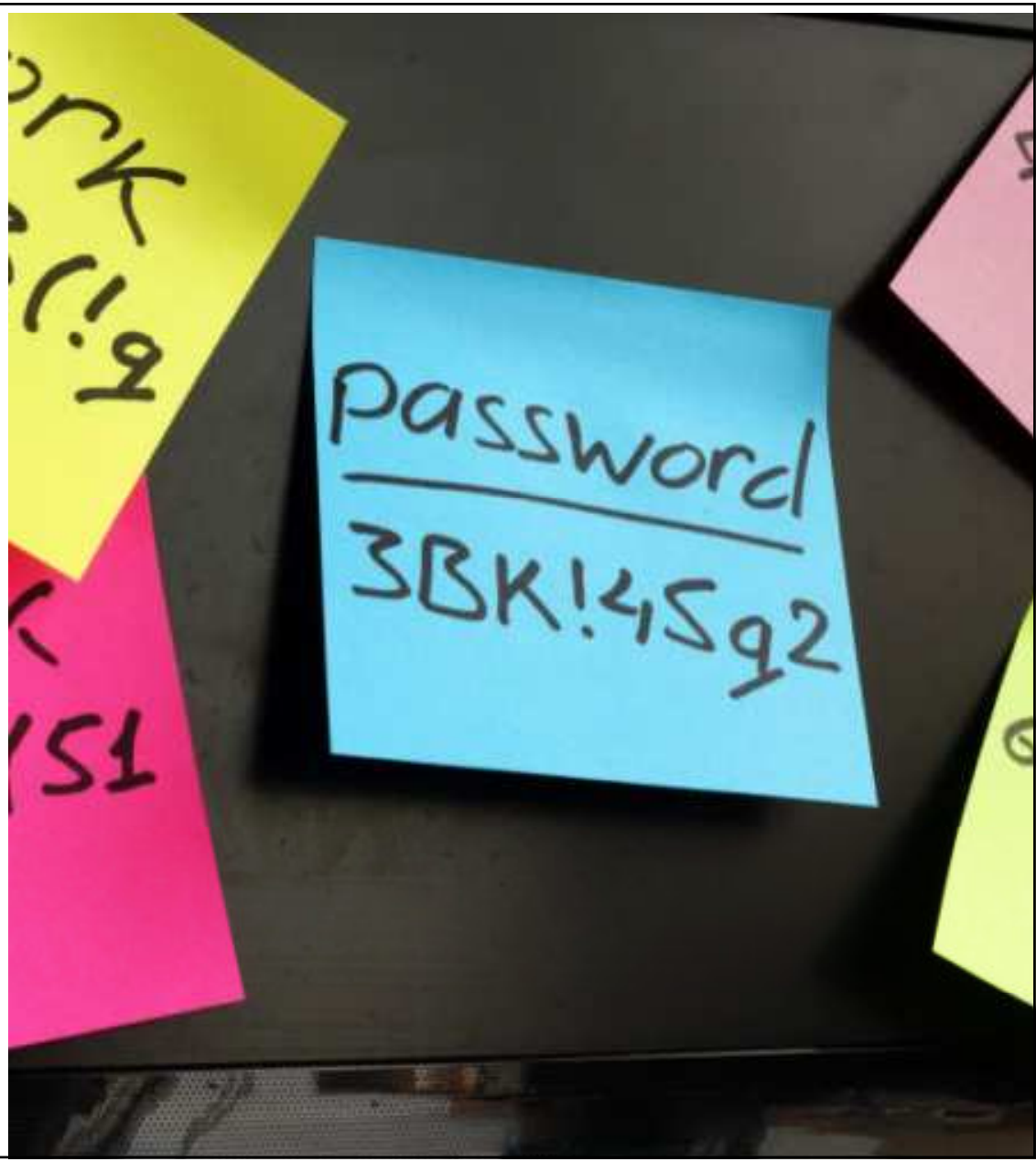
Kyberhygiena

- Hesla
- Zabezpečení zařízení
- (Ne)bezpečí na síti
- Bezpečnost e-mailové komunikace
- Digitální identity

MUNI
ICS

Hesla

- Základní mechanismus autentizace
- Heslem prokazujeme svou identitu
- Hesla odemykají naše informace a tajemství
- Hesla skrývají nejen informace o nás, ale často i o našich blízkých



Poznáte silnější heslo?

R52@n0F&

BotaTancujePolku

Poznáte silnější heslo?

R52@n0F&

8 hodin

BotaTancujePolku

2 biliony let

Bezpečná hesla = Frázová hesla

- Pro lidský mozek lehce zapamatovatelná a jedinečná hesla pro každého
- Základ frázového hesla:
  - část básně
  - scenérie cestou do práce, školy či výletu
  - vzpomínka z dětství
  - pořekadlo či říkanka
  - hláška z oblíbeného filmu
- Na délce záleží = aspoň 3 slova!

Prolomitelnost hesel

1. Sociální inženýrství – prozradíme je sami
2. Útok hrubou silou – „uhádne“ je specializovaný SW

- Sdílení hesel s ostatními osobami
- Opakování hesel
- Jednoduše odvoditelná hesla (jména domácích mazlíčků či dětí)
- Seznam hesel „na papíru“ přilepeném na monitoru v kanceláři

MUNI
ICS

Správce hesel

- On-line či off-line trezor našich hesel (nejenom)
- Chráněno jedním „hlavním a silným“ heslem
- Možnost volby různorodých či generovaných hesel

- **OS Windows:** Bitwarden, LastPass, KeePass, NordPass, Keeper
- **OS Linux:** Bitwarden, LastPass, KeePassX(C), Buttercup, Keeper
- **Mac OS X:** Klíčenka, 1Password, LastPass, DashLane, Keeper

Vícefaktorové ověřování

- MFA – Multi-Factor Authentication
- Často známé a používané „Dvoufaktorové ověření – 2FA“
- Další „pokročilejší“ vrstva ochrany proti prolomení hesel
- Klíčové pro ochranu “důležitých“ účtů
- Eliminace většiny útoků a přitom stačí udělat jen o krok navíc

Vícefaktorové ověřování

MUNI
ICS

Vícefaktorové ověřování

- Faktor znalosti (něco, co znáte) – kombinace uživatelského jména a hesla, PIN, jednorázové OTP (One-time password) hesla nebo bezpečnostní otázky
- Faktor vlastnictví (něco, co máte) – jiné důvěryhodné zařízení, platební karta nebo bezpečnostní hardwarový token.
- Faktor biometrie (něco, co jste) – otisk prstu či ucha, sken očnice, rozpoznání obličeje či hlasu, obraz krevního řečiště

Biometrie

- Budoucnost vícefaktorového ověřování
  - Otisk prstu, sken obličeje, oční sítnice, krevního řešiště, autentizce ucha (neinvazivní)
  - Další výzkum primárně v oblasti otisků prstů
- Problémy zneužití
  - Padělky otisků prstů – možné vyrobit i v domácím prostředí či jednoduše sejmout
  - Autentizace za pomoci fotografie (digitalizovaný obraz tváře)
- Problémy revokace
  - Biometrické údaje na celý život – revokace prstu či ucha???
  - Prozatím řešeno generováním sady šablon jedinečných pro jednotlivce

Překonané metody*

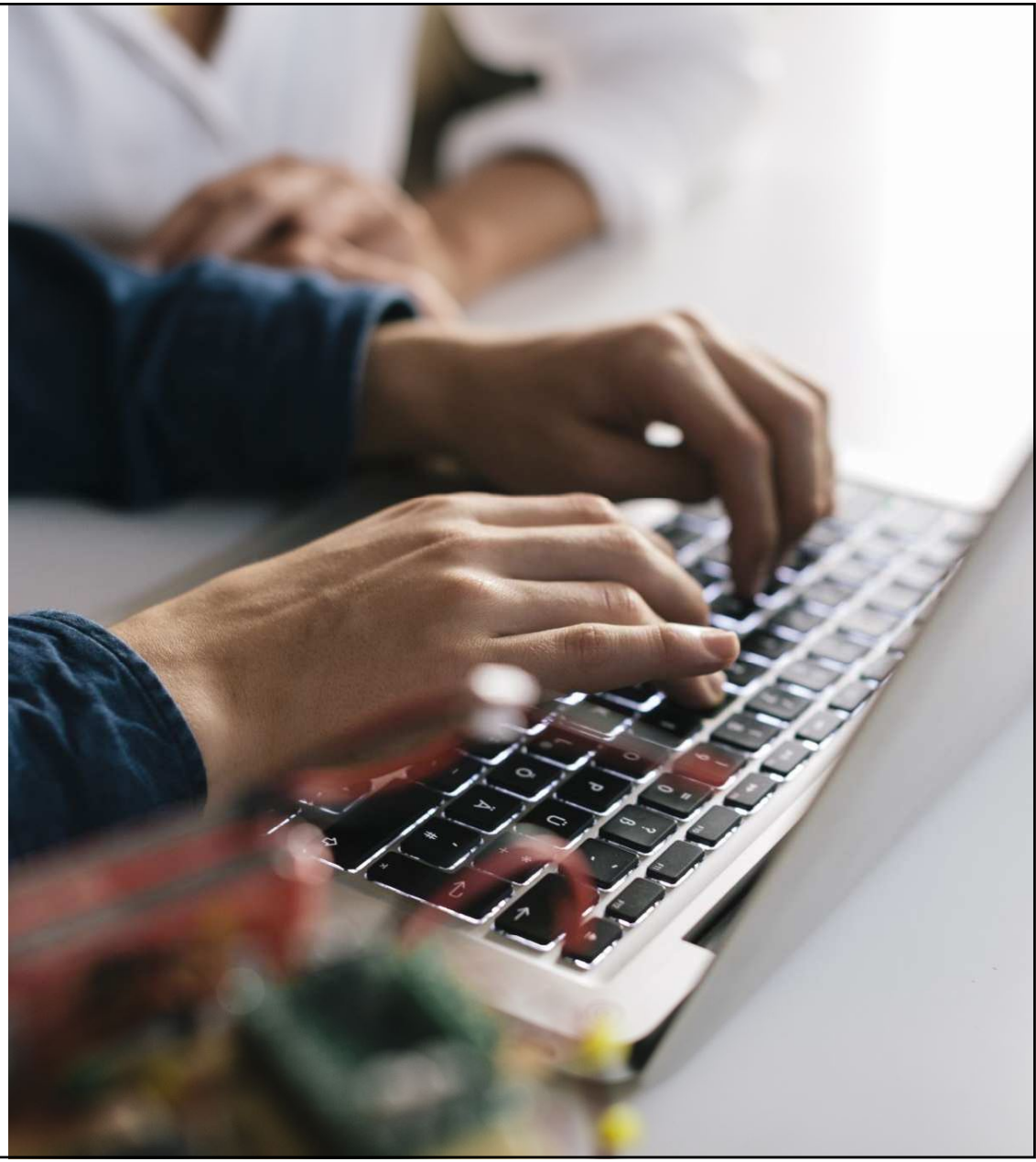
- Zapisovat hesla na papírky či si je pamatovat nazpaměť
- Pravidelně měnit heslo (např. 180 dnů)
- Hlídat dříve nastavená hesla (5 posledních)
- Nahrazovat písmena speciálnymi znaky nebo čísly (@#$~^1234)
- 100% spoléhat na bezpečnost hesla

*dle doporuční NIST (National Institute of Standards and Technology)

MUNI
ICS

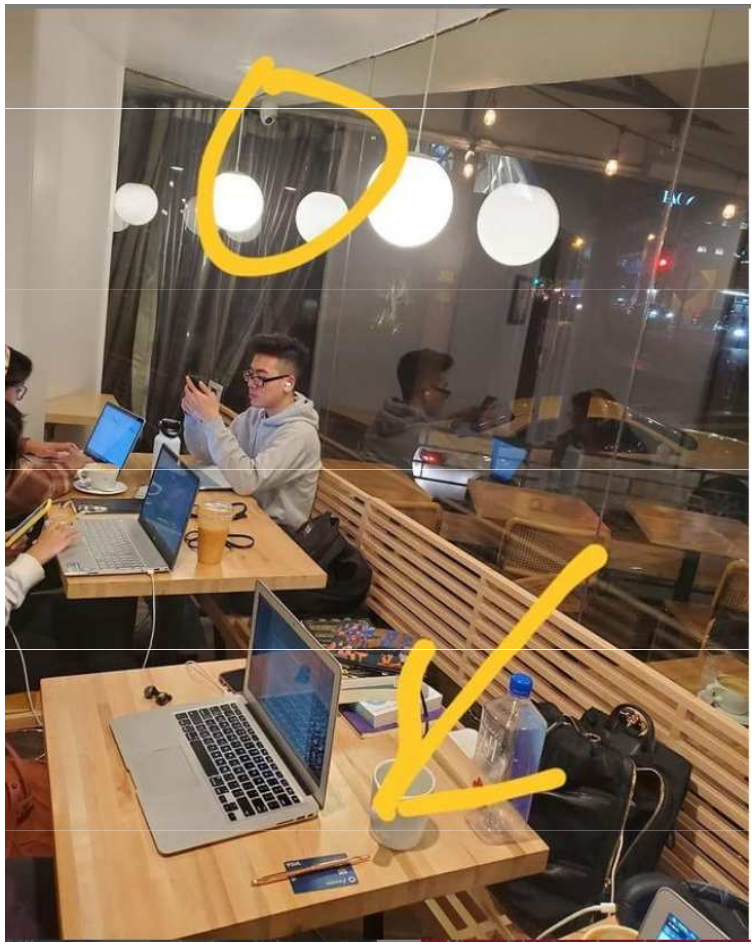
Zabezpečení zařízení

- Zařízení jsou branou do světa internetu
- Preventivní návyky jsou účinná zbraň
- Z maličkostí se dá udělat účinná ochrana



Co je na této fotografii špatně?

Co uživateli reálně hrozí?



MUNI ICS

Uzamykání obrazovky mobilního zařízení

- Výrazně **snižuje riziko zneužití dat** či zařízení
- Heslo do zařízení je základním prvkem ochrany před vniknutím či ovládáním
- Metody pro **odemčení u chytrých telefonů**:
  - PIN, heslo
  - kreslená gesta
  - biometrický zámek (otisk prstu – TouchID, rozpoznání obličeje – FaceID)
- Nejméně a nejvíce bezpečná metoda odemykání obrazovky?
- U počítačů se používá ruční zamykání obrazovky pomocí klávesových zkratek
  - Windows klávesa + L (OS Windows), Controle + Command + Q (Mac OS X)

Náhledy notifikací

- Dokáží **komukoliv poblíž odhalit** naše soukromí
- U mobilních zařízení prozrazují **více informací, než je zdrávo**
  - A to nejen při odcizení
- Poškozují obrazovky u mobilních zařízení
- Kompromisem je nastavit si náhled pouze na jméno osoby
  - Nejčastěji u SMS či IM zpráv
- V případě počítače řešení pomocí zamykání obrazovky

Antivirové řešení

- Dnes již **komplexní bezpečnostní řešení**
  - Antivir, Antispam, Antispyware, Antimalware, Rezidentní ochrana, Firewall, Spouštění aplikací
- Síto na **odfiltrování nebezpečí** (nejen) internetu
- Detekují podezřelé soubory, SW, malware, síťový provoz, externí disky
- **Nutnost aktualizace** AV databáze
- Nejznámější výrobci AV řešení:
  - Microsoft Defender, ESET, AVAST, F-Secure, Kaspersky, Bitdefender

Pravidelné aktualizace

- **Přijdou vždy, když se to nejméně hodí a jsou otravné!**

- Poskytují ale vyšší bezpečnost vašeho SW i HW
- Opravují chyby, zkrášlují nebo vylepšují služby prostřednictvím instalace nejnovějších verzí softwaru
- Klíčové je neotálet a dělat je pravidelně

Testované zálohy

- **Jak nepřijít o svá data i v případě krádeže, ransomware nebo poško zení zařízení?**

- Využít on-line nástroje:
  - OneDrive
  - Google Drive
  - Apple iCloud

To nejdůležitější:

- Je dobré zálohovat důležité soubory, protože o ně můžeme lehko přijít.
- Kromě nečekaného selhání pevného disku nás může ohrozit i ransomware.
- Ransomware zašifruje naše data a za přístup k nim bude žádat výkupné.
- Když máme data někde zálohována, bolí nás tahle nepříjemná situace méně.
- Zálohovat se dá do cloudu (OneDrive atp.) nebo lokálně (externí pevný disk atp.
- Občas je dobré také zálohy otestovat, že fungují.

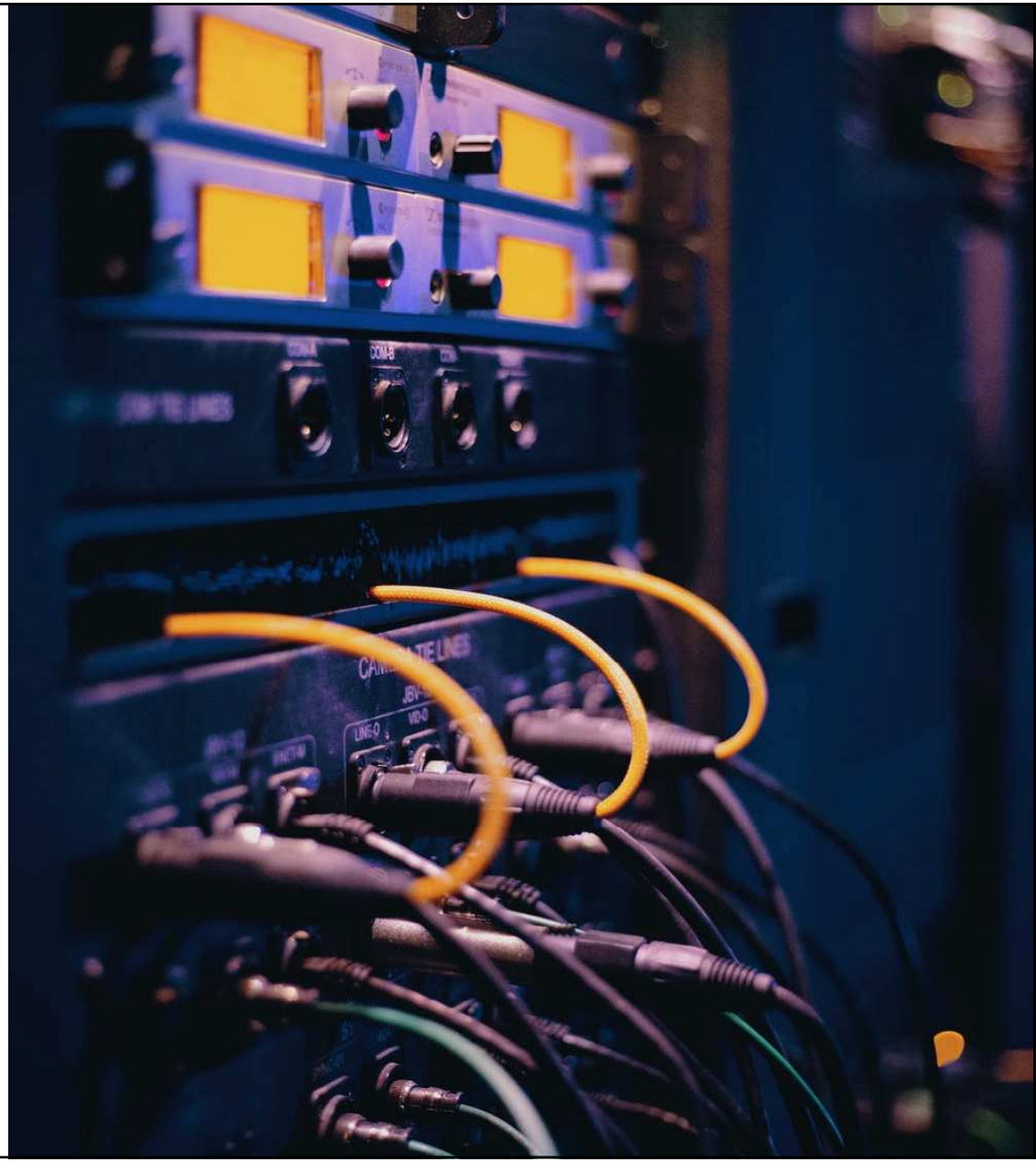
Ztráta zařízení

- Co dělat v případě ztráty?
  - Volat o pomoc? Volat kamarádovi? Volat Policii ČR? Nevolat?
- Ideálně využít on-line služby „Najdi moje zařízení“:
  - Vzdáleně zabezpečí zařízení (vymažou data, vyfotí zloděje)
  - Nechají telefon vyzvánět
  - Zobrazí jej na mapě
  - **Najdi moje zařízení (pro Android)**
  - **Najít můj iPhone (pro iOS)**

MUNI
ICS

(Ne)bezpečí sítí

- Nejde jen o to, dostat se na internet, ale dostat se tam bezpečně
- Ne každá WiFi síť je stejná
- Ne každá WiFi je bezpečná
- Nebezpečí veřejných WiFi sítí



Veřejné WiFi sítě bez hesla

- Velké bezpečnostní riziko pro citlivé údaje a data
- Lovení obětí pomocí “fakových” veřejných WiFi v nákupních centrech, kavárnách či letištích
- Na WiFi bez hesla Vás vidí všichni připojení (a že je jich hodně)
- Není obtížné získat vaše hesla, data či údaje o kreditní kartě
- Dobré je vypnout funkci automatického připojování na dostupné WiFi bez hesla

Veřejné WiFi sítě s heslem

- O něco bezpečnější pohyb na internetu
- Vidí Vás jen legitimně připojení uživatelé (lepší než nic)
- Nicméně data jsou stále čitelná/odchytnutelná pro připojené uživatele
- Správu nad sítí má pouze administrátor dané sítě
- Jste si jisti čistými úmysly správce? :)

Virtuální privátní síť (VPN)

- Pomyslný tunel do „bezpečné“ sítě
- Dovnitř VPN útočník neuvidí jen tak nevidí
- Zajišťuje bezpečné připojení odkudkoliv, i z veřejné WiFi sítě
- Typicky poskytovaná služba zaměstnavatelem nebo i VVŠ
- VPN na MUNI – https://it.muni.cz/sluzby/vpn

Eduroam

- Jedná se o bezpečné připojení a máme i na MUNI!
- WiFi infrastruktura provozovaná mezinárodní výzkumnou a vzdělávací komunitou
- Dostupný celosvětově, a dokonce ne nutně v okolí tamější akademické půdy
- Aby Eduroam fungoval jak má, je třeba instalace konfiguračního nástroje Eduroam CAT

MUNI
ICS

Bezpečnost e-mailové komunikace

- E-mail = hlavička a tělo
- Šifrování a digitální podpis
- Kritické myšlení při podezřelých e-mailech

Jak je to s těmi e-maily?

From: e-mailová adresa odesílatele

To: adresa příjemce

Cc: kopie e-mailu, kde může být více adres oddělených čárkou

Bcc: skrytá kopie

Reply-To: adresa pro odpověď. Pokud není žádná zadána, použije se adresa z „From“

In-Reply-To: identifikuje předcházející korespondenci

Subject: předmět zprávy

Date: datum a čas odeslání zprávy

Message-ID: ID e-mailu, které je automaticky generováno mail serverem

Received: jednotlivé položky identifikující servery, přes které e-mail prošel. Jako první položka je cílová stanice (Váš počítač) a poslední je zdrojová (odkud byl e-mail poslán), tedy chronologicky lze cestu sledovat od poslední položky k první.

Elektronický podpis

- Zajišťuje **integritu a nepopiratelnost** přenášené zprávy a odesilatele
- Elektronický podpis garantuje, že **zprávu odesíláte opravdu vy** a že zpráva **nebyla během přenosu změněna**
- Nahrazuje klasický vlastnoruční podpis
- Realizován za pomoci osobního certifikátu X.509 či PGP klíče

Šifrování

- Zajišťuje **důvěrnost** přenášené zprávy
- Zprávu si **nepřečte nikdo kromě legitimního příjemce**
- Zpráva se převádí z čitelného textu na nečitelný šifrovaný text, který může dešifrovat jenom „skutečný“ příjemce
- Zajišťuje oblast kryptografie – symetrická či asymetrická

Kritické myšlení při podezřelých e-mailech

ZAČNĚTE SI UŽÍVAT NOVOU PLATFORMU PHIL.MUNI.CZ, ABYSTE SE VYHNULI ZTRÁTĚ SVÉHO ÚČTU PRO WEBMAIL. KLIKNĚTE ZDE [1] PRO OVĚŘENÍ VAŠÍ NOVÉ PLATFORMY PHIL.MUNI.CZ PODLE POKYNŮ ADMIN HELP DESK, POKUD NEBUDE DO 24 HODIN OVĚŘENA, BUDOU VŠECHNY ZPRÁVY DORUČENÉ POŠTY SMAZÁNY A VÁŠ WEBOVÝ ÚČET BUDE UKONČEN.

PODPORA
VEDENÍ TÝMU
PHIL.MUNI.CZ © COPYRIGHT

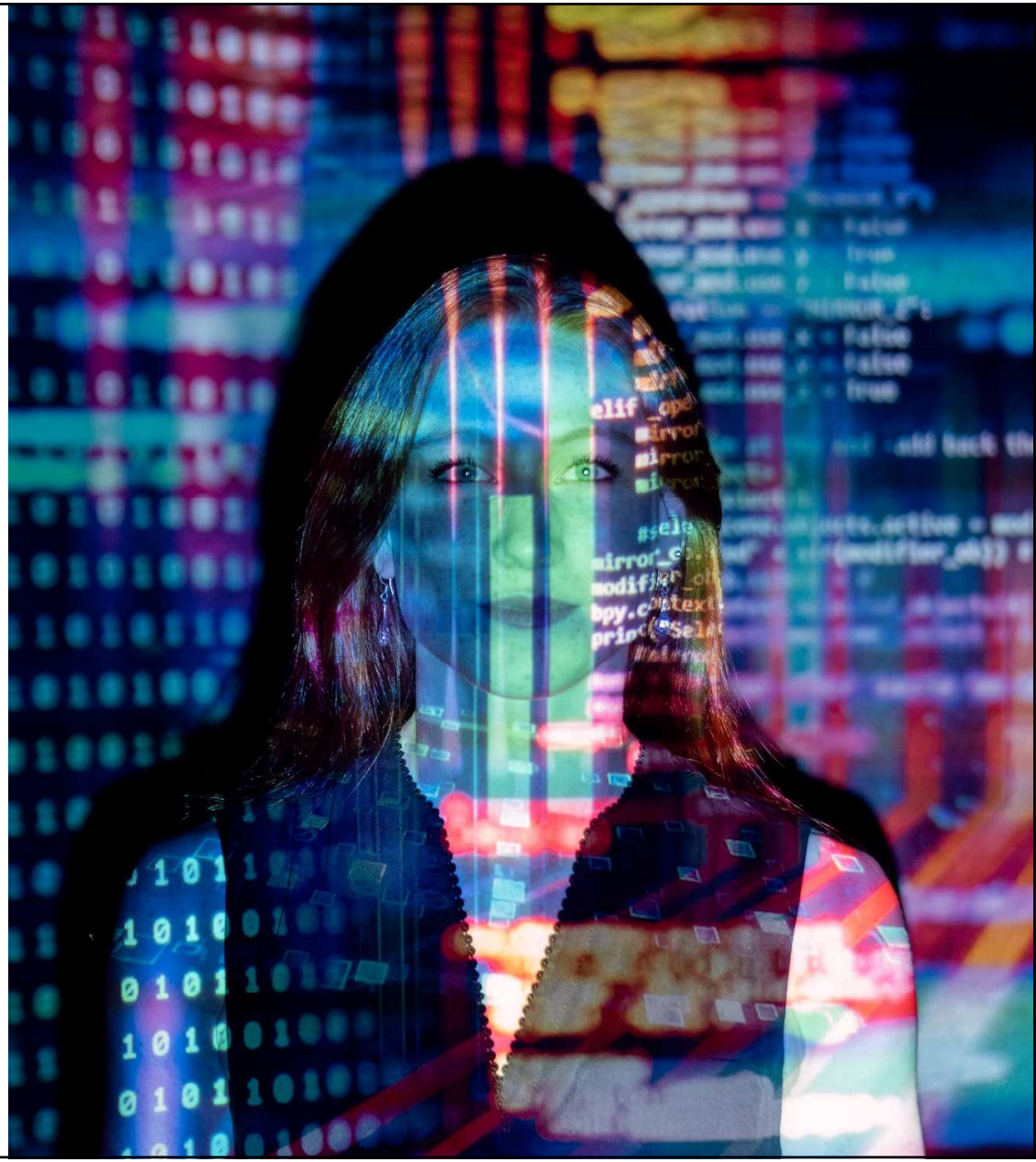
Links:
---
[1] http://mailphilmunizsquirrelmailsrcloginph9.mw.lt/

MUNI ICS

MUNI
ICS

Digitální identita

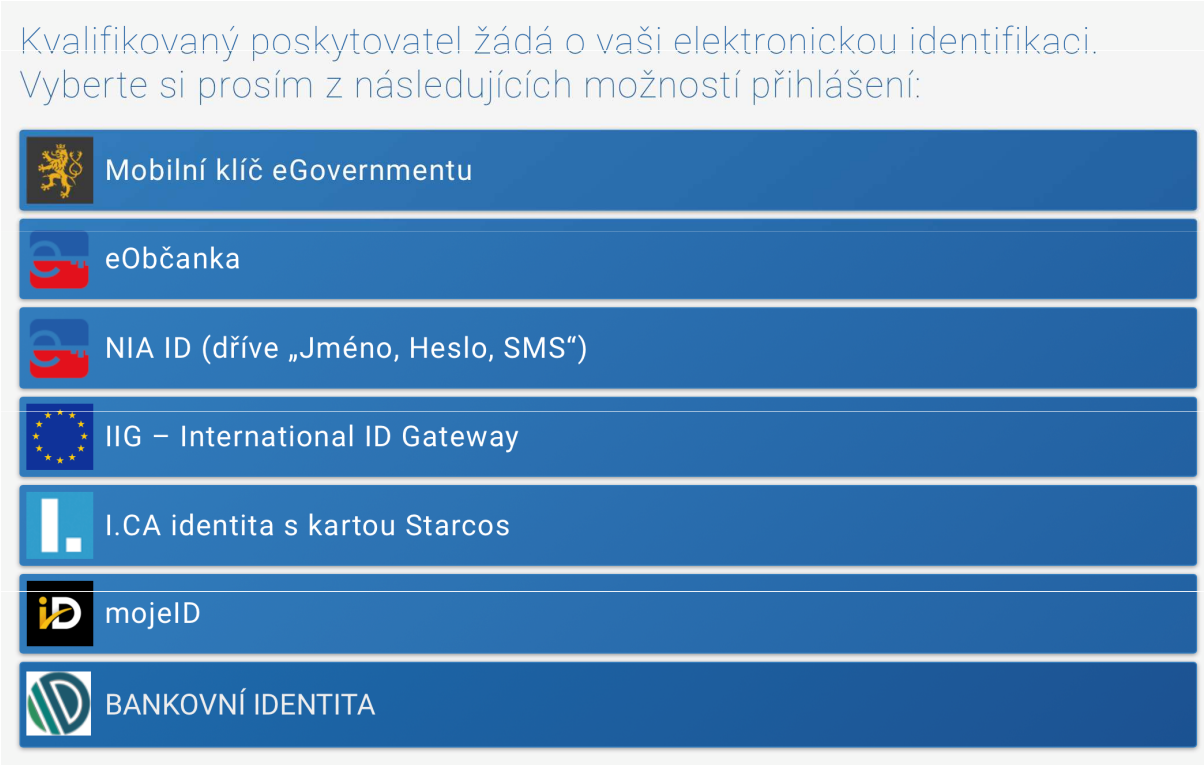
- Vzniká na základě digitální stopy
- Reflektuje nás a naše chování v online světě
- Slouží jako vstupní brána do IS



Digitální stopa

- Vytváříte ji **veškerou svou činností** ve virtuálním prostředí
- V dnešní době je už téměř nemožné se ji vyhnout
- Vědomé vs. nevědomé sdílení informací
  - Historie prohlížení, cookies, zakoupené produkty, navštívená místa s GPS, sociální sítě
  - Ani s anonymním prohlížečem nejsme neviditelní
- Vždy dobře zvažujte co umístíte na sociální sítě
  - Za pár let to bude zajímat HR oddělení
- Toto vše pak tvoří Vaší digitální identitu
  - Je velmi cenná, soukromá a dá se s ní velmi dobře obchodovat

Elektronická identita



MUNI ICS

Závěrečná úvaha

Jen pozor na češtinu:
"Čím vyšší..., tím víc"

„Čím vyšší rizika plynou ze zneužití systému nebo služby, tím je nutné aplikovat silnější bezpečnostní opatření.”

„Používejte selský rozum a buďte zdravě nedůvěřiví!“

Chcete se dozvědět více?

- Stránky CSIRT-MU – https://csirt.muni.cz
- Bezpečnostní portál MUNI – https://security.muni.cz
- Kurz Kyberkompas
- Kurz GDPR
- Techniky sociálního inženýrství
- Projekt CRP-KYBER21

MUNI
ICS

Děkujeme za pozornost

MUNI
CSIRT-MU