MUNI
ICS

Kyberbezpečnost

Tomáš Plesník et al.

CSIRT-MU, 29. 11. 2023

Co nás v rámci této části čeká?

Kyberhygiena

- 1. přednáška – 29. 11. 2023
- Jak se bránit *(„Těžko na cvičišti…“)*

Kybernetické útoky

- 2. přednáška – 6. 12. 2023
- Čemu se bránit (*„Lehko na bojišti!“)*

Závěrečná esej

- Připravena celkem 4 témata

MUNI ICS

Představení

Tomáš Plesník (přednášející)

- Vedoucí Divize kyberbezpečnosti a správy dat, ÚVT MU
  - Manažer KB MU dle zákona č.181/2014 Sb. (ZoKB)
  - Správce zabezpečeného IS dle zákona č. 412/2005 Sb.
- Řešitel (mezi)národních projektů v oblasti KB
- Koordinátor projektů v oblasti KB v prostředí VVŠ
- Držitel ceny Ceny ministra vnitra za mimořádné výsledky v oblasti bezpečnostního výzkumu – projekt „Kybernetický polygon“
- Konzultant v oblasti kybernetické a informační bezpečnosti
- https://csirt.muni.cz/about-us/team-members

MUNI ICS

Slovník zkratek

- NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost
- NCKB – Národní centrum kybernetické bezpečnosti
- ZoKB/ZKB – Zákon o kybernetické bezpečnosti
- VoKB/VKB – Vyhláška o kybernetické bezpečnosti
- KII – Kritická informační infrastruktura
- ISZS – Informační systém základní služby
- VIS – Významný informační systém
- PZS – Poskytovatel základní služby
- VoVIS/VVIS – Vyhláška o VIS
- OSS – Orgány státní správy
- OVM – Orgány veřejné moci

- **ISMS – Information Security Management Systém (SŘBI)**
- **SŘBI – Systém řízení bezpečnosti informací (ISMS)**
- **KB – Kybernetická bezpečnost**
- **BI – Bezpečnost informací**
- **IT – Informační technologie**
- **IS – Informační systém**
- **ICT – Informační a komunikační technologie**
- **APT – Advanced Persistent Threat**
- **TTPs – Tactics, techniques and procedures**
- **ERP – Enterprise Resource Planning**

Doporučená literatura

- DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
- KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
- KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.
- PAČKA, Roman. CSIRT: v přední linii boje proti kybernetickým hrozbám. Brno: Centrum pro studium demokracie a kultury, 2019. Politologická řada. ISBN 978-80-7325-473-5.
- SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.
- NÚKIB, NAKIT, MVČR, 2023. Minimální bezpečnostní standard [*online*]. 3. vyd. [*cit. 13. 4. 2023*]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf
- ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Zákony pro lidi.cz [*online*]. © AION CS 2010-2021 [*cit. 10. 4. 2023*]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181
- ČESKO. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: Zákony pro lidi.cz [*online*]. © AION CS 2010-2021 [*cit. 10. 4. 2023*]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82
- ČESKO. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: Zákony pro lidi.cz [*online*]. © AION CS 2010-2021 [*cit. 2. 4. 2023*]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412
- 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.
- ČSN EN ISO/IEC 27000:2020 (36 9790) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Přehled a slovník. Praha: Český normalizační institut, 2020.
- ČSN EN ISO/IEC 27001 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnostiinformací – Požadavky
- ČSN EN ISO/IEC 27002 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatřeníbezpečnosti informací
- ČSN P ISO/IEC TS 27100:2021 (369771) Informační technologie – Kybernetická bezpečnost - Přehled a pojmy. Praha: Český normalizační institut, 2020.

MUNI ICS

Disclaimer

Cybersecurity

⇔*

Kybernetická bezpečnost

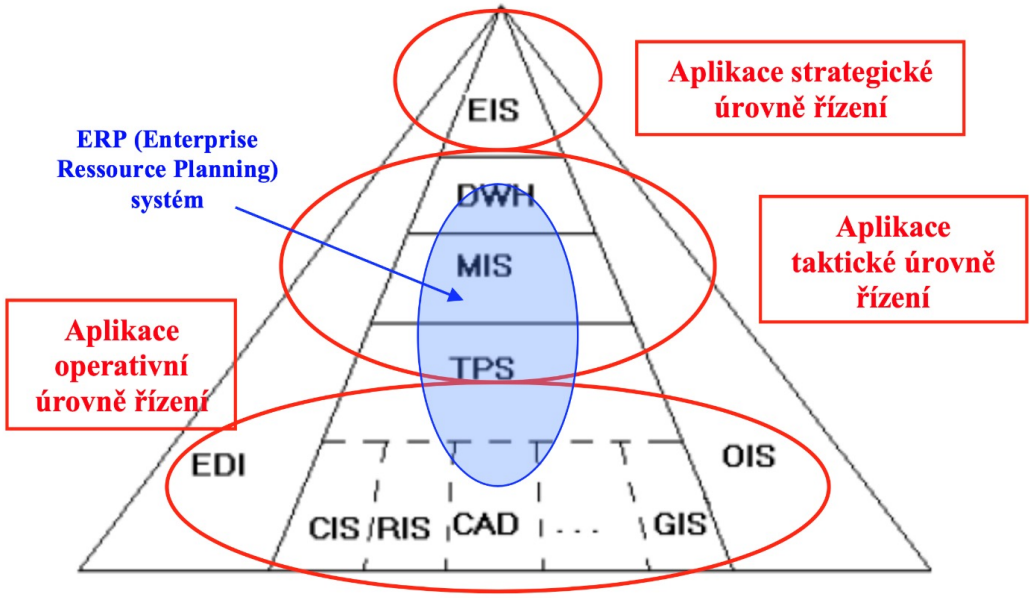
⇔*

Kyberbezpečnost

(* alespoň v rámci této přednášky)

ICT/IS v organizacích

- ICT infrastruktura – standardní
  - Servery, domény, počítačové sítě, služební počítače, přenosná zařízení
  - Webové aplikace (služby), elektronická pošta, datová úložiště, cloud
  - Osobní počítače a zařízení (BYOD)
  - Tiskárny, kopírovací stroje, skenery, faxy
  - Čtečky karet, kiosky, informační tabule, rezervační systémy
- Státní či veřejné organizace – specifické
  - Základní registry státu, Spisová služba, Úřední deska,
  - Informační systémy stavebního či životního prostředí
  - Registr smluv, Registr veřejných zakázek, Registr zpracování OÚ
- Soukromé společnosti – specifické
  - EIS – strategické
  - ERP (DWH, MIS, TPS), CRM, OIS, EDI – taktické
  - CIS, RIS, CAD, GIS, EDI – operativní



MUNI ICS

Evropská unie

TOP 5 nejzasaženějších sektorů:

1. Veřejná správa/vláda ← ← ←
2. Poskytovatelé digitálních služeb
3. Široká veřejnost
4. Zdravotnictví
5. Finance a bankovnictví

Zdroj: ENISA: European Union Agency for Cybersecurity (2021)

MUNI CSIRT-MU

Evropská unie

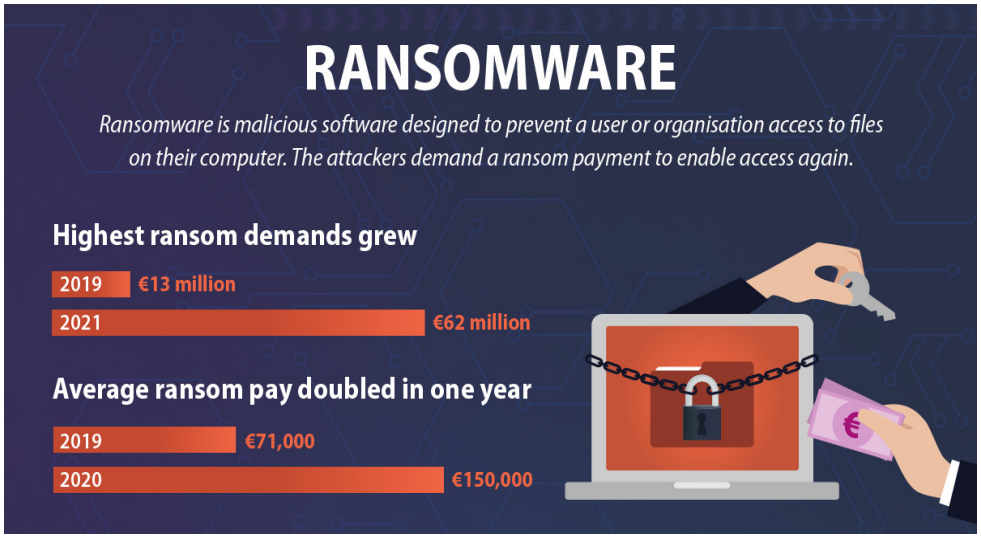
Zdroj: ENISA Threat Landscape (ETL) report – 9th edice z roku 2021

TOP 10 nejčastějších útoků:

1. Ransomware
2. Malware
3. Cryptojacking
4. Hrozby související s elektronickou poštou
5. Hrozby související s daty
6. Hrozby proti dostupnosti a integritě
7. Dezinformace
8. Neškodlivé hrozby
9. Útoky na dodavatelský řetězec

MUNI CSIRT-MU

Evropská unie



Zdroj: ENISA: European Union Agency for Cybersecurity (2021)

Růst požadavků na výkupné:

- 2019 – 13 mil. €
- 2021 – 62 mil. €

49 mil. €/2 roky

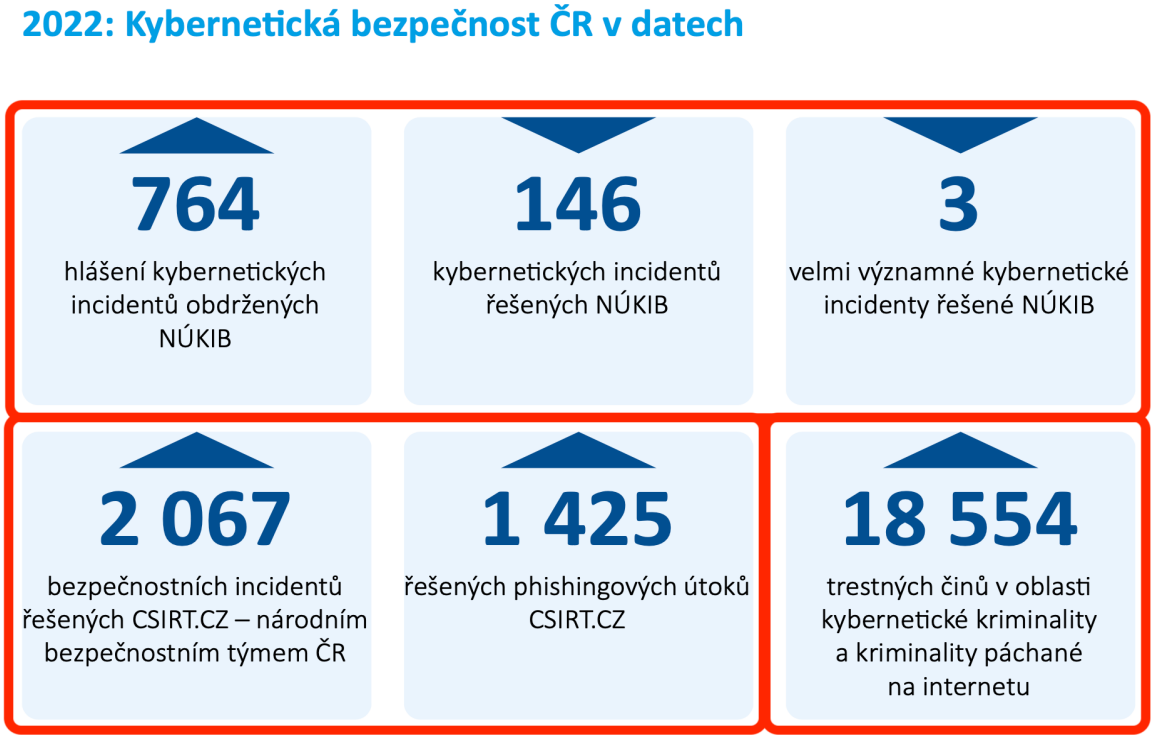
Průměrná výše výkupného:

- 2019 – 71 tis. €
- 2020 – 150 tis. €

79 tis. €/1 rok

MUNI CSIRT-MU

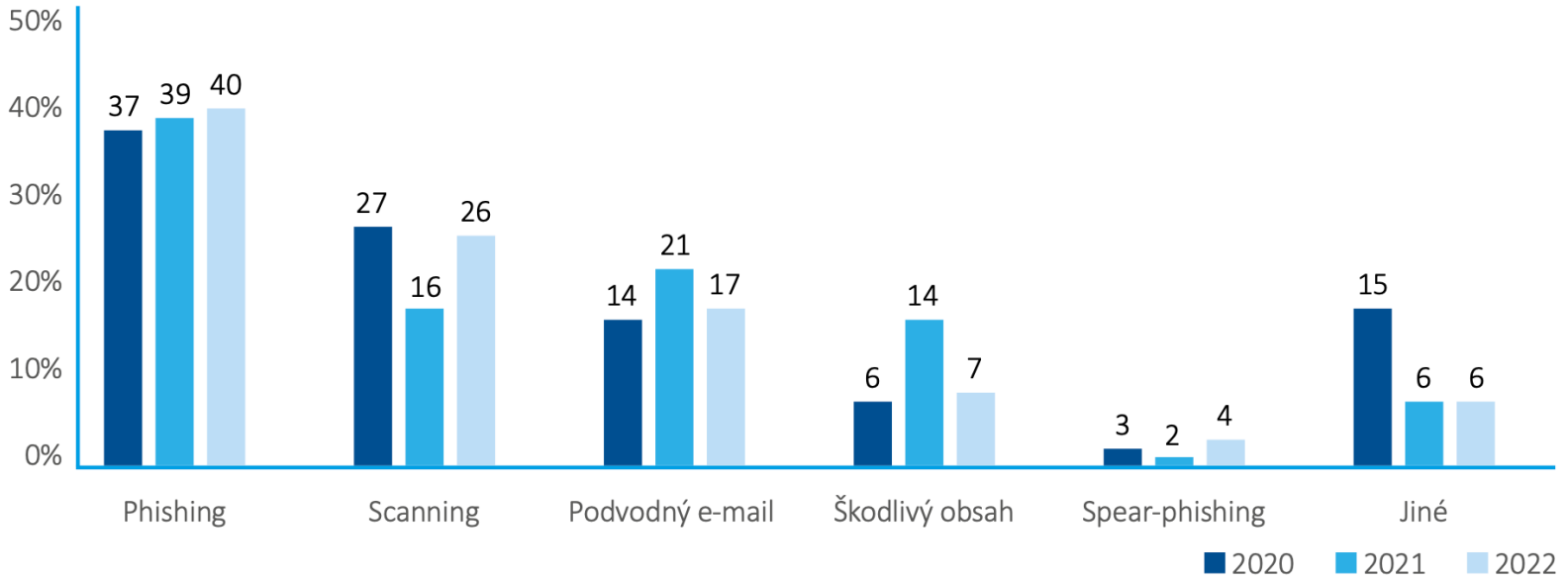
Česká republika



Zdroj: Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022

MUNI ICS

Česká republika

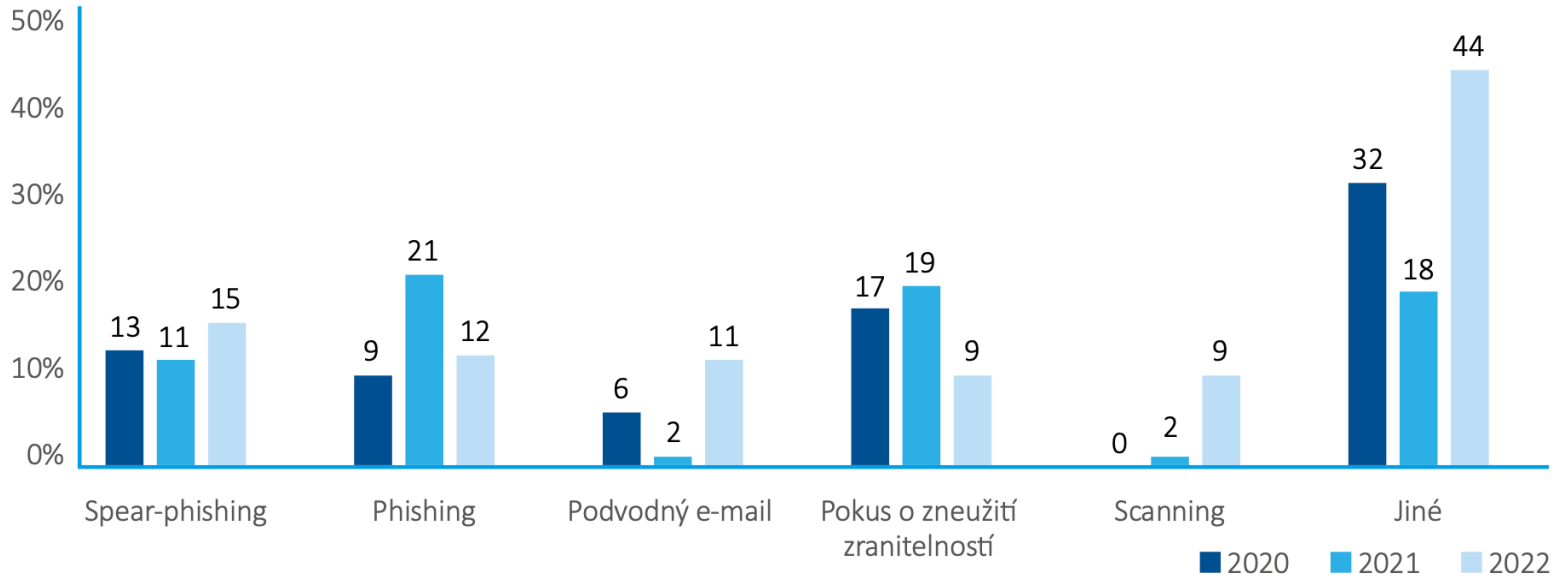


Graf 4: Kategorie nejčastějších typů kybernetických útoků v letech 2020–2022 (% respondentů)

Zdroj: Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022

MUNI ICS

Česká republika



Graf 5: Kategorie nejzávažnějších typů kybernetických útoků v letech 2020–2022 (% respondentů)

Zdroj: Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022

MUNI ICS

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 + krizové situace a s nimi související trendy** – home-office a distanční formy výuky

---

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

Motivace

Motivace

- Březen 2013 – DDoS útoky na zpravodajské weby, Seznam.cz, Dopravní podnik hl. m. Prahy
- Prosinec 2019 – ransomware Emotet - Trickbot - Ryuk v OKD (> 5 mil. Kč)
- Prosinec 2019 – ransomware Emotet - Trickbot - Ryuk v nemocnici v Benešově (>50 mil. Kč)
- Březen 2020 – Ransomware Defray ve FN Brno (>150 mil. Kč)
- Březen 2021 – KB útok tři soukromé polikliniky v centru Prahy
- Březen 2021 – KB útok na pražský magistrát, MPSV a SŽDC
- Duben 2021 – Ransomware Avaddon na Magistrátu města Olomouc
- Květen 2021 – Ransomware v Národní knihovně
- Únor 2022 – DDoS na weby MV ČR, Policie ČR
- Březen 2022 – KB útok na el. systémy na Úřad městské části Praha 5, Praha 9 a Praha 1
- Duben 2022 – KB útok Městský úřad Žďáru nad Sázavou
- Duben 2022 – DDoS na weby MV ČR, ČD (Killnet)
- Květen 2022 – ransomware na Ředitelství silnic a dálnic (ŘSD)
- Září 2023 – ransomware na Univerzitu obrany (UNOB)

Masarykova univerzita

- **Zvyšující se počty KB událostí a incidentů**
  - Událost (pokus o útok) → automatizovaná detekce
  - Incident (reálný útok) → manuální reakce
- **2019**: **111 317** událostí
  - **541** incidentů
- **2020**: **121 387** událostí (**nárůst o 9 %**)
  - **1 591** incidentů (nárůst o 194 %)
- **2021**: **147 949** událostí (**nárůst o 22 %**)
  - **1 388** incidentů (pokles o 12 %)

MUNI ICS

Definice

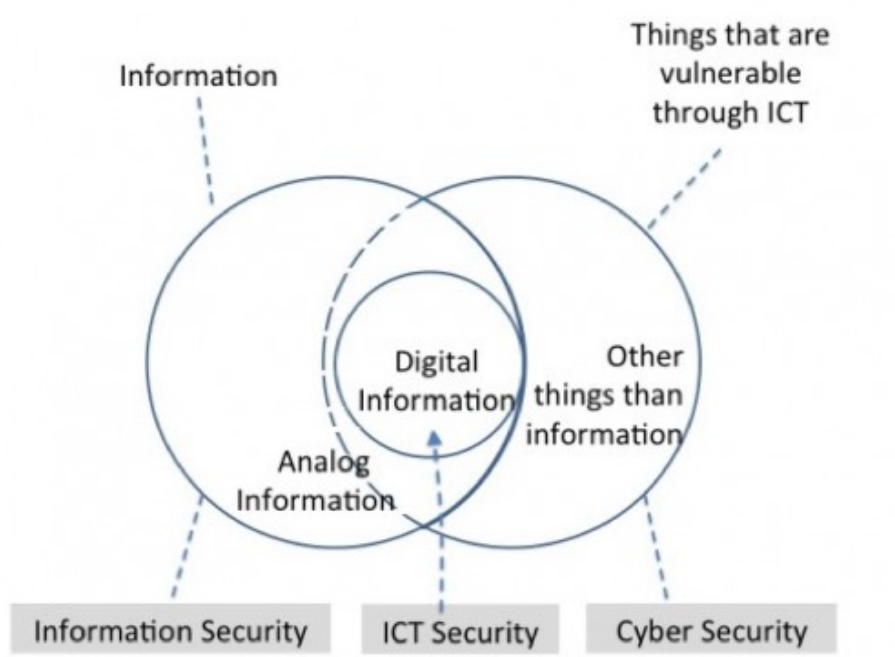
Kybernetická bezpečnost

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

* Kyberprostor – Summit NATO ve Varšavě uznal kybernetický prostor jako pátou operační doménu již v roce 2016.

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.

Definice



Zdroj: Center for Cyber and Information Security (https://ccis.no/cyber-security-versus-information-security/)

1. Informační bezpečnost

   (Information security)

2. Kybernetická bezpečnost

   (Cyber Security)

3. Bezpečnost informačních a komunikačních technologií

   (ICT Security)

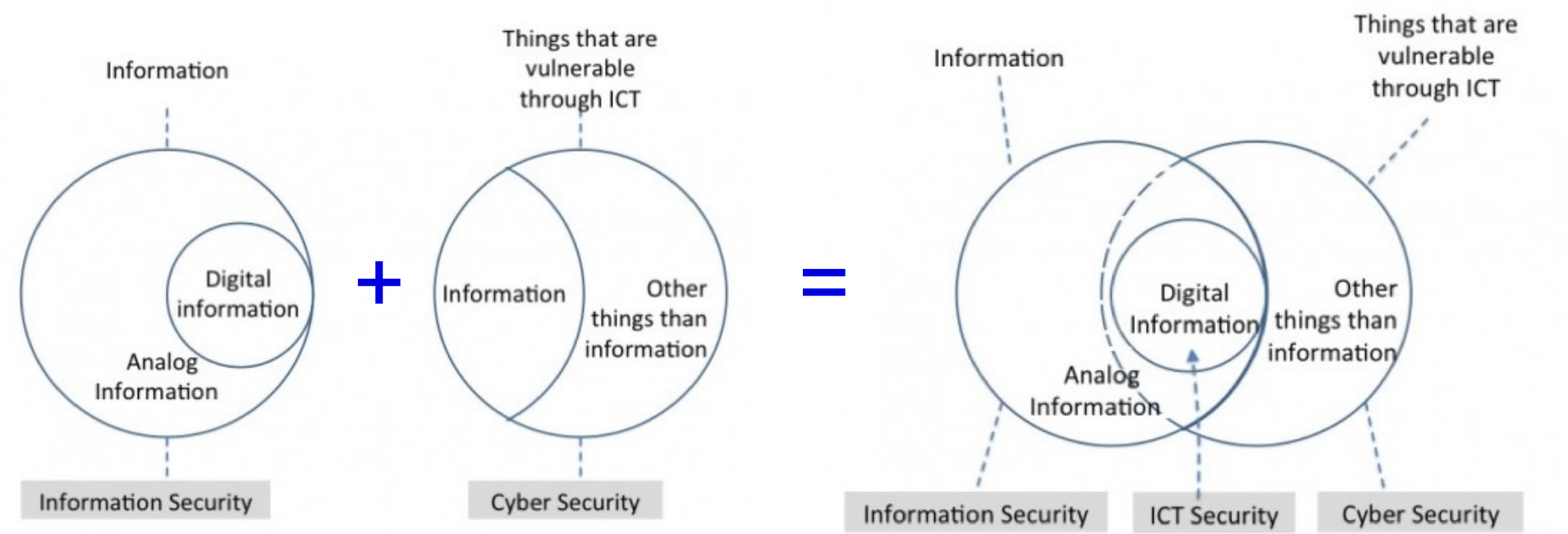
MUNI ICS

Informace

Data	• Fakta, údaje (znakové řetězce)
Informace	• **Data spolu s jejich významem (databáze)**
Znalosti	• Informace vzájemně související (znalostní báze)

MUNI ICS

Kybernetická nebo informační bezpečnost?



Zdroj: Centre for Cyber and Information Security at the Norwegian University of Science and Technology

MUNI CSIRT-MU

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 transkripce do ZoKB v Q2/2024
- **Vyhláška č. 82/2018 Sb. Vyhláška o kybernetické bezpečnosti (VoKB)**
  - Na základě normy ISO/IEC 27001 (ISMS – Requirements) – zavedení SŘBI v organizaci
- **Regulace z pohledu národní autority – NÚKIB**
  - Systémy KII, ISZS a VIS
  - **Na MUNI celkem 2 VIS – IS MU a EPIS MU**

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 tak složité a mnohdy nic nestojí**

MUNI ICS

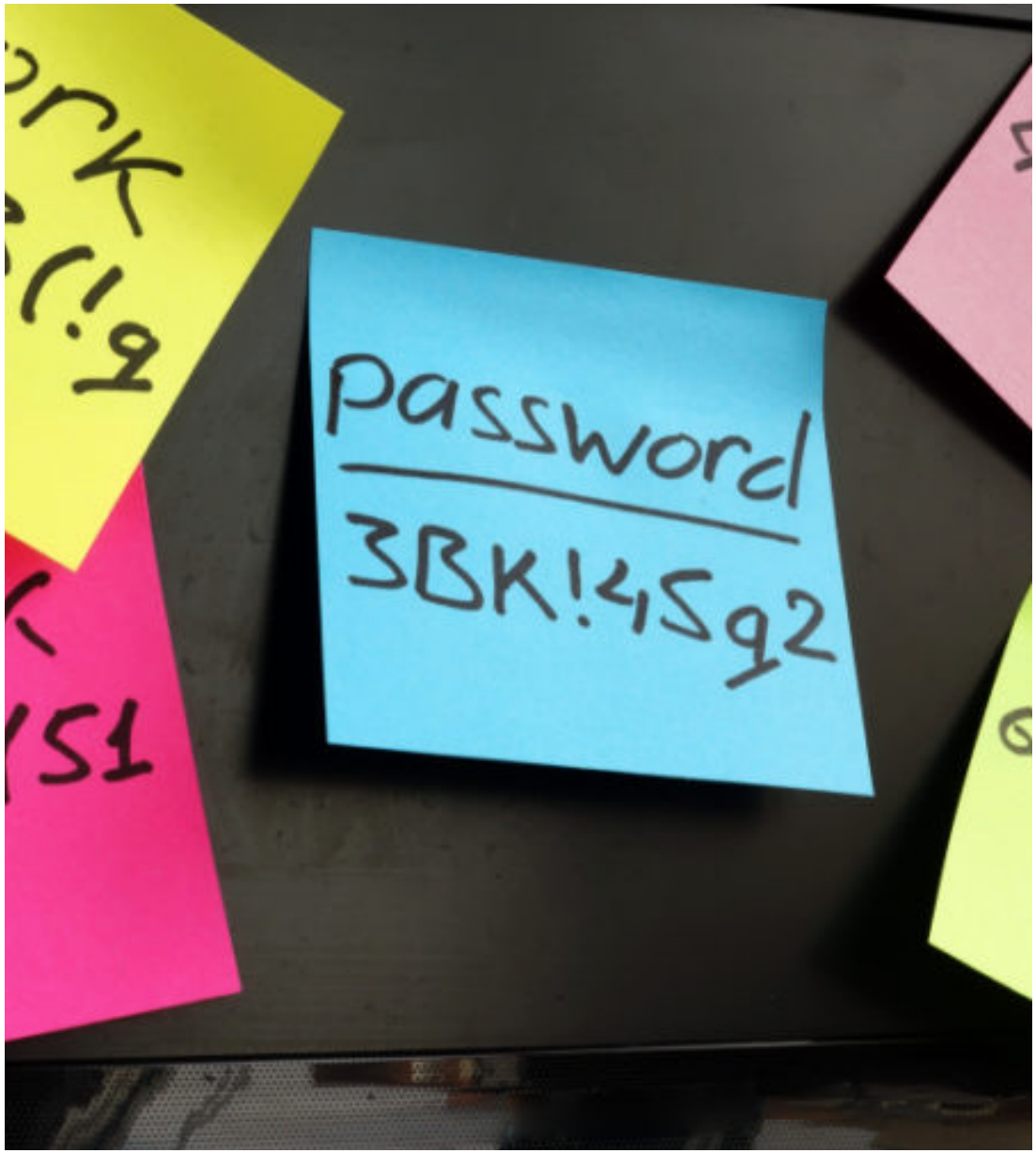
Kyberhygiena

- 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

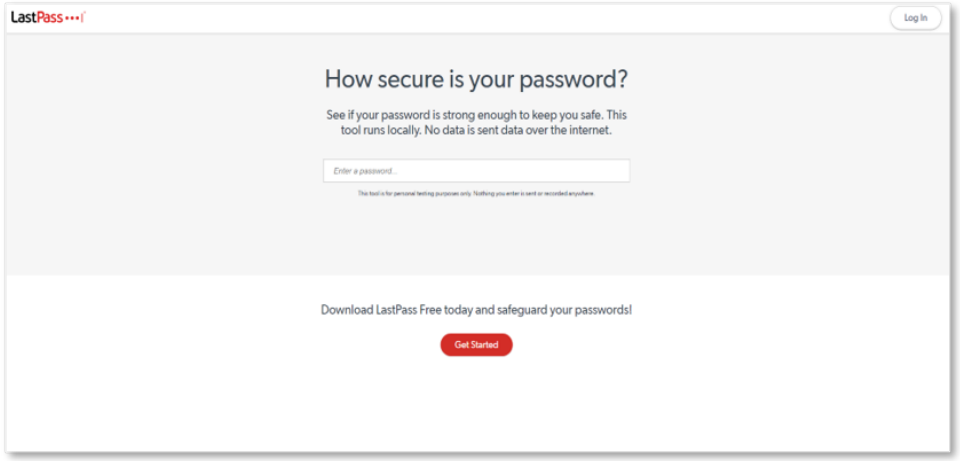
MUNI ICS

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 až 4 slova!
  - Ukázka: *trhatfialkyB00Mdynamitem, H0OPskočilzajícpřes2pole, 3karatovýprstenodM., 10%šancevsázcesPetrem, 8_polibšosKosům, třistaTřicet3stříbrných, GdeD0movmůj...*

MUNI ICS

Síla hesel



Nikdy nezadávejte své pravé heslo!

MUNI ICS

Prolomitelnost hesel

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

- Sdílení hesel s ostatními osobami
- Opakování hesel, využívání zástupných znaků
- Začíná velkým písmenem, končí číslicí,
- Jednoduše odvoditelná hesla (jména domácích mazlíčků či dětí)
- Používání jednoho hesla k více službám
- Seznam hesel „na papíru“ přilepeném na monitoru v kanceláři

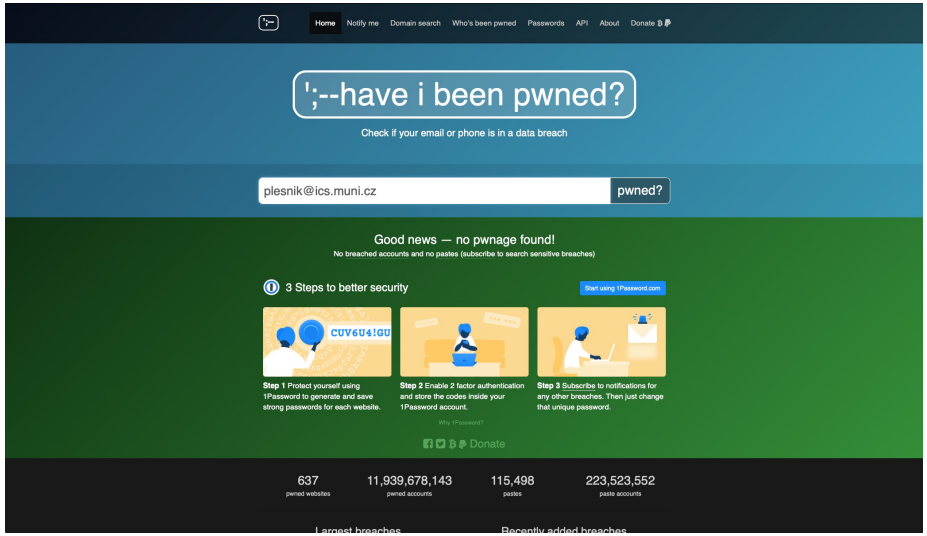
MUNI
ICS

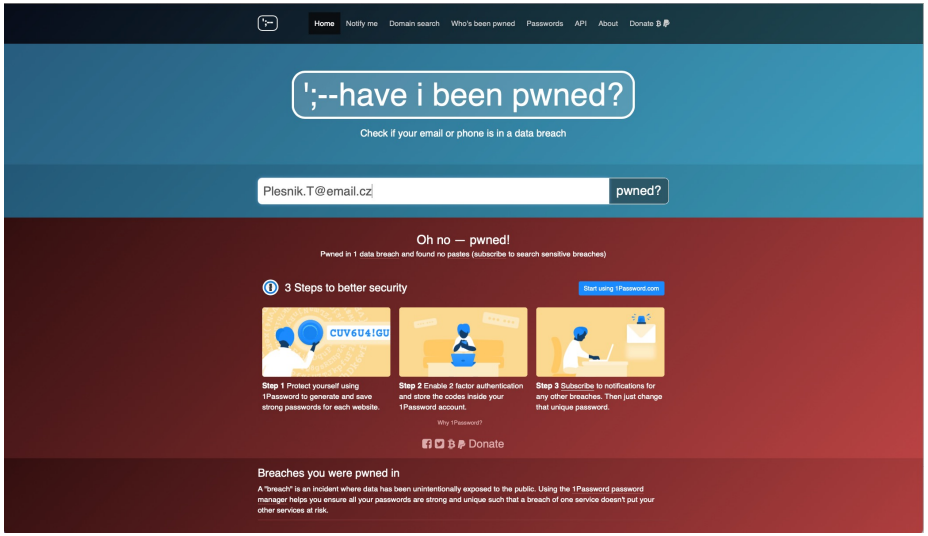
Správce hesel

- 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

Únik přihlašovacích údajů





Zdroj: https://haveibeenpwned.com

MUNI ICS

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
- Pletení si SSO (Single-Sign-On) se sdílením jednoho hesla k mnoha službám

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

MUNI ICS

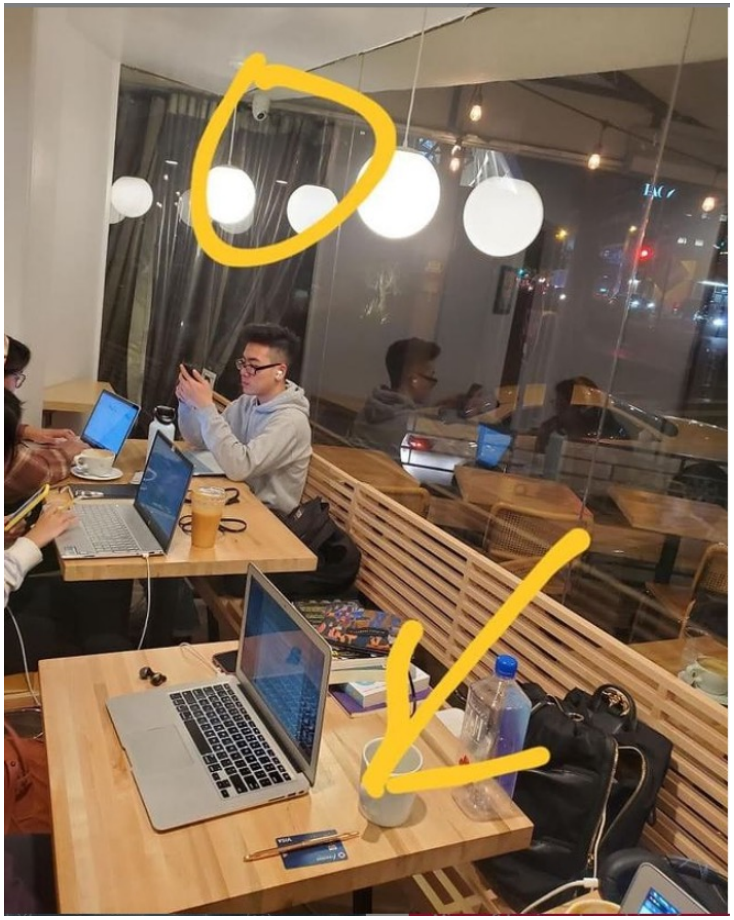
MUNI
ICS

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), Control + 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

Zálohování + 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.

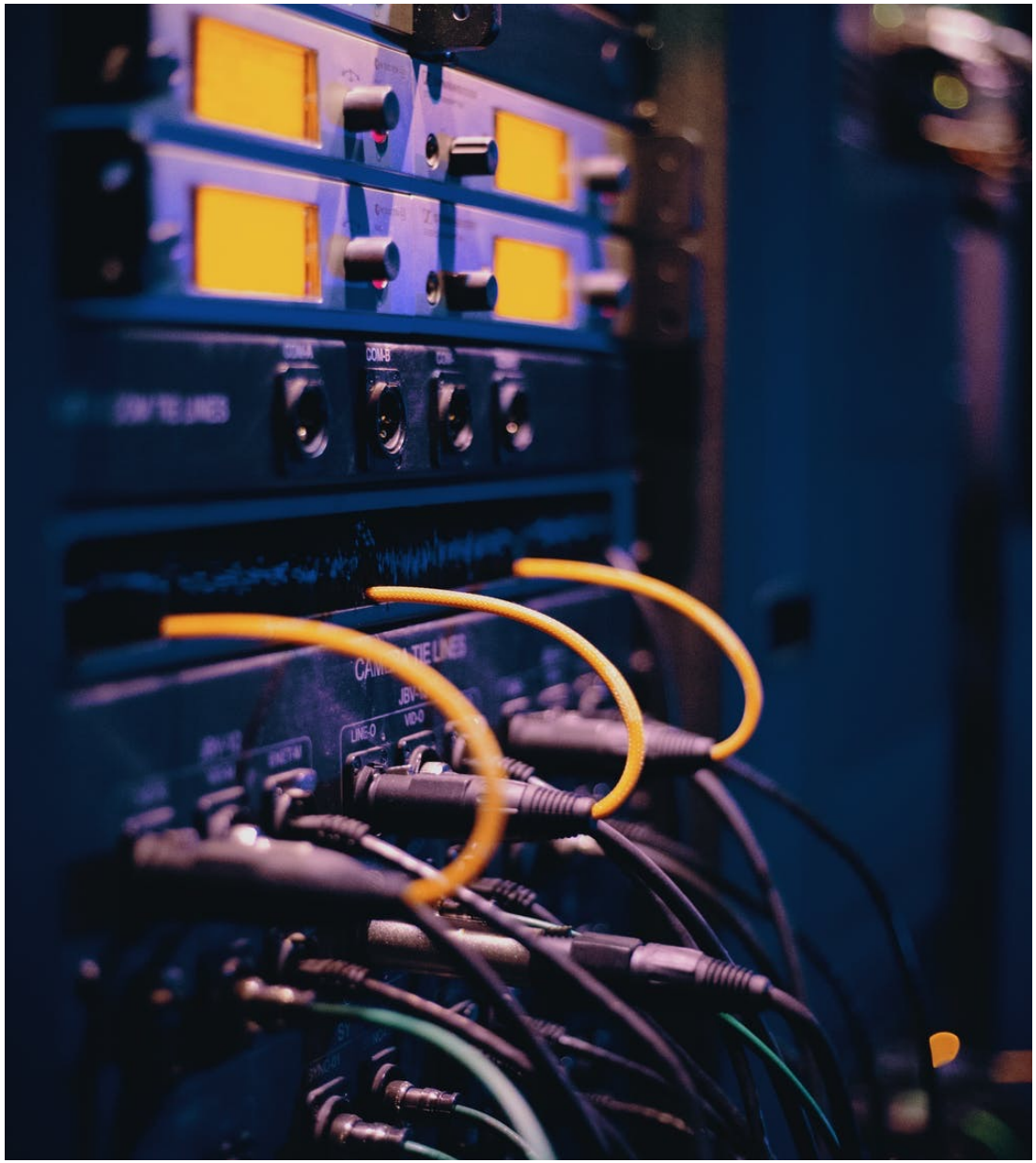
Ztráta zařízení

- 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)**

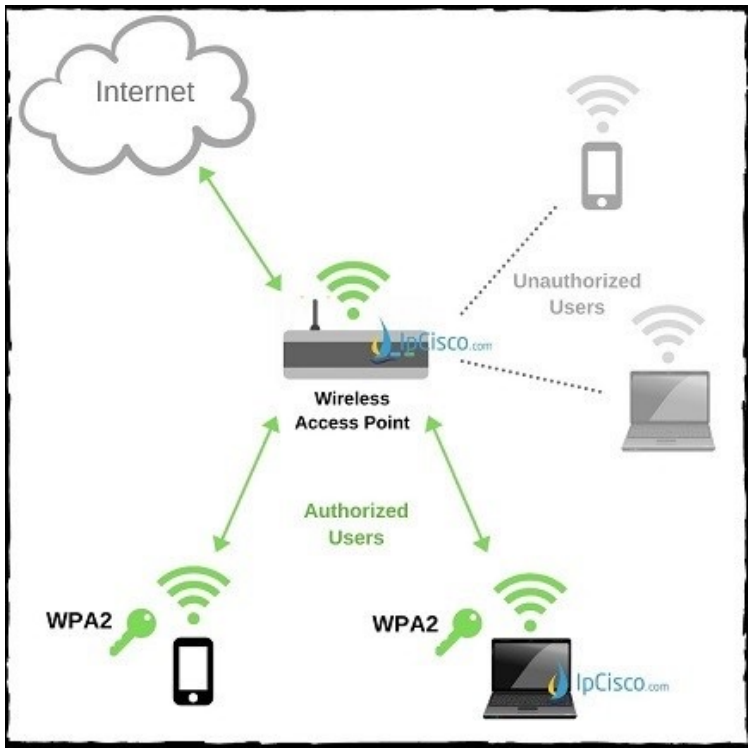
MUNI
ICS

(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

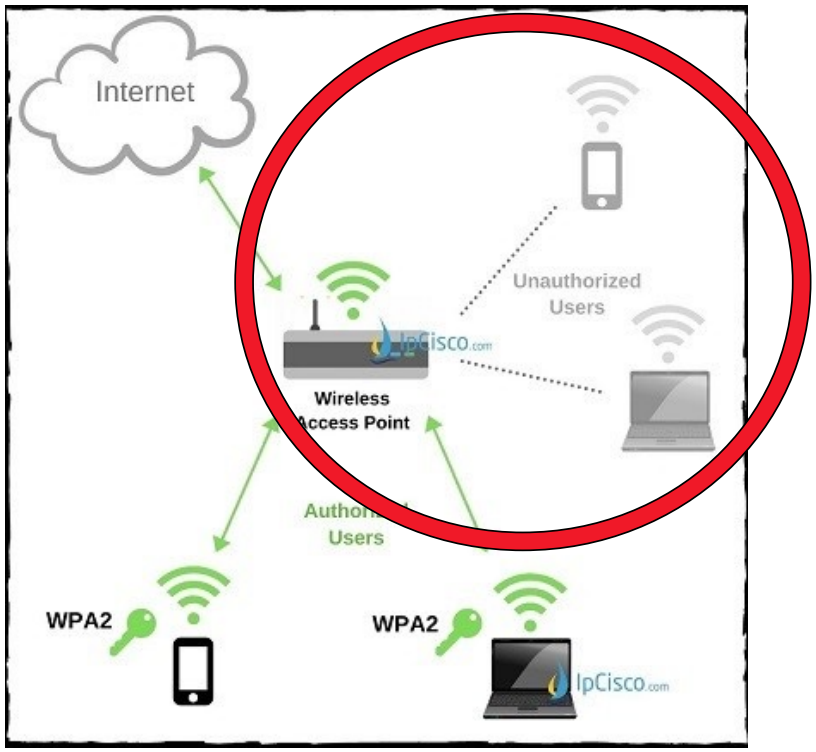


Koncept WiFi sítě



MUNI
ICS

Veřejné WiFi sítě bez hesla

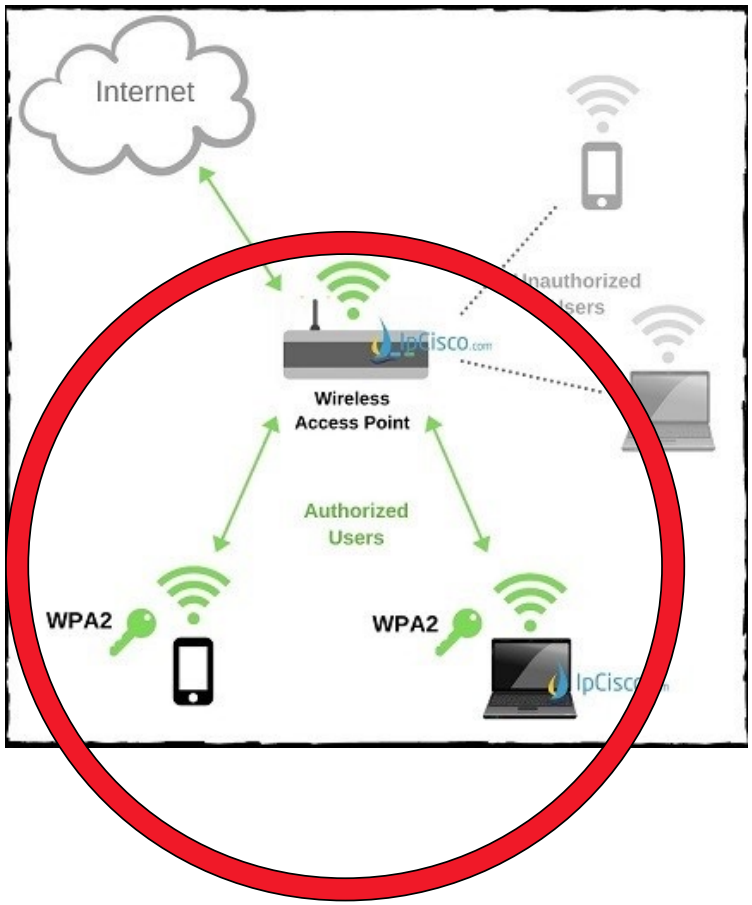


MUNI
ICS

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

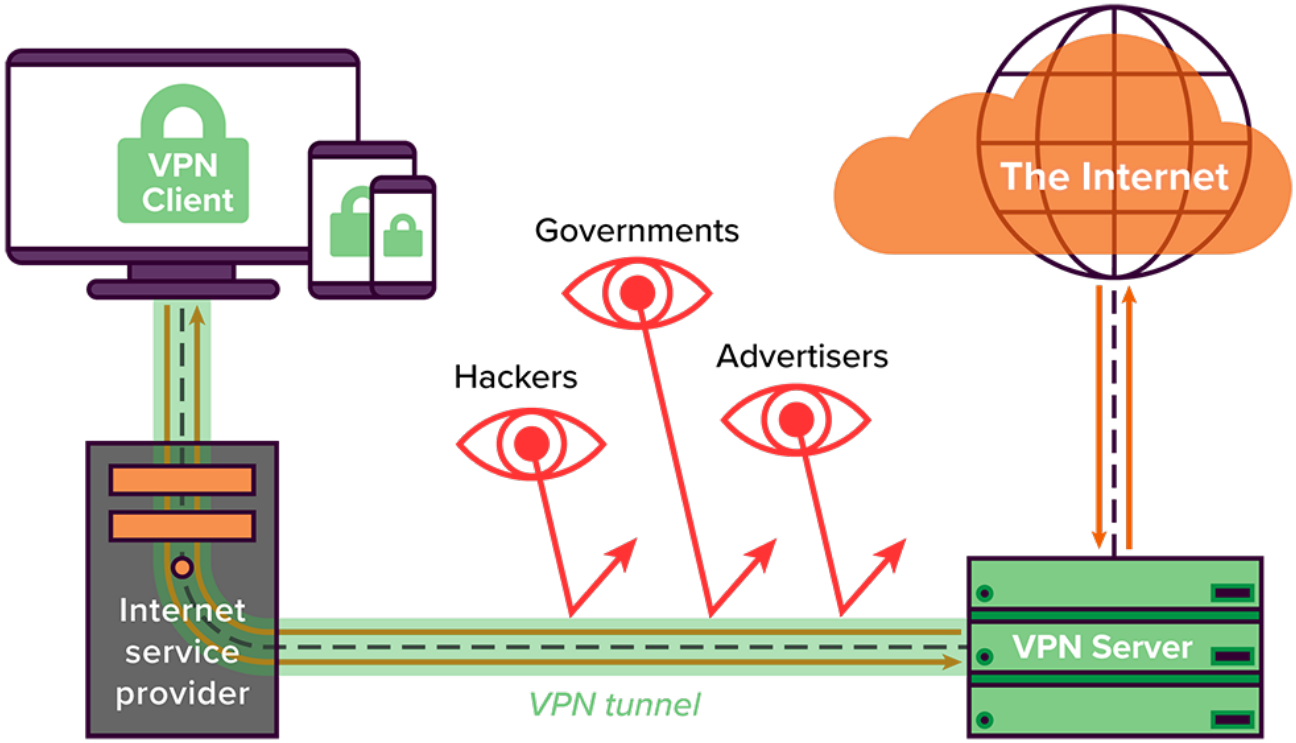


MUNI
ICS

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)



MUNI ICS

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
- Autentizace poskytována RADIUS serverem domácí organizace
  - Připojuji se na University of Barcelona, ale autentizuji se na MUNI
- 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

MUNI
ICS

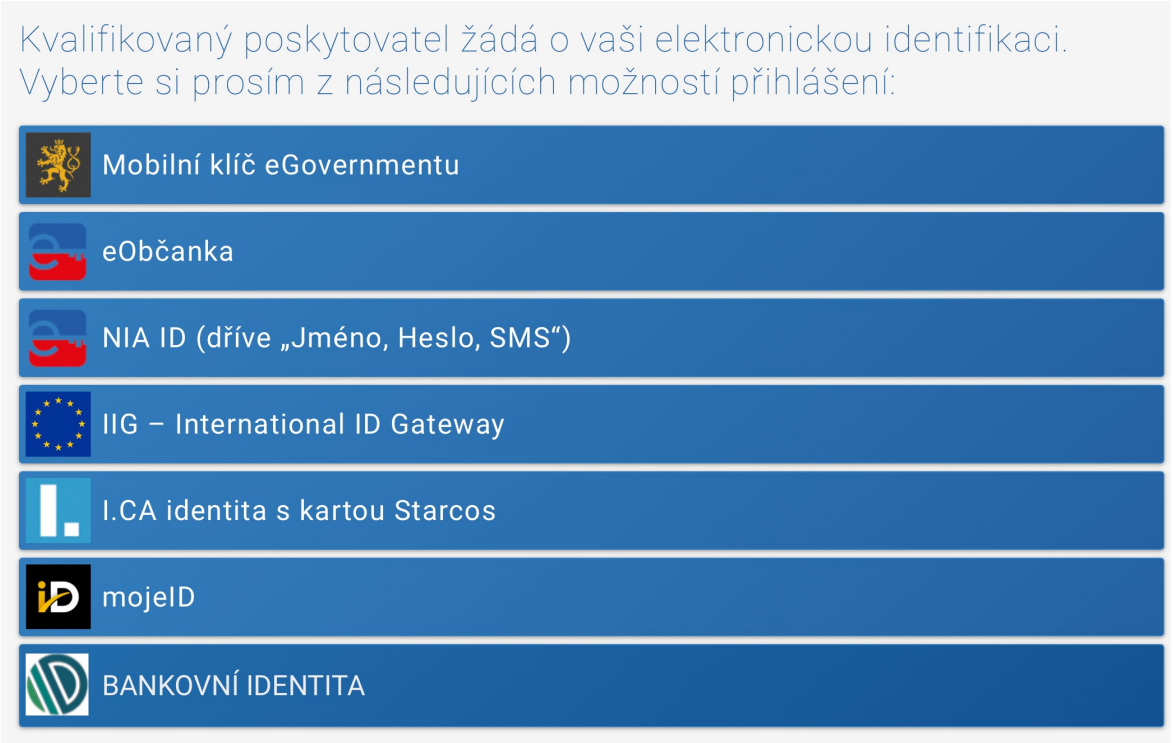
Digitální identita

- 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

MUNI
ICS

Závěrečná úvaha

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

“Používejte selský rozum a buďte zdravě nedůvěřivý!”

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-KYBER

MUNI ICS

MUNI
ICS

Děkuji za pozornost

MUNI
CSIRT-MU