

# Základy bezpečného chování na Internetu, aneb jak se nenechat odposlouchávat

Viktor Ferus - WEBnet Incident Response Team

[ferusvi@civ.zcu.cz](mailto:ferusvi@civ.zcu.cz)

[www.viktor-ferus.cz](http://www.viktor-ferus.cz)

Centrum Informatizace a výpočetní techniky



# Motivace, aneb já nemám, co skrývat

- ▶ Časté reakce při debatách o bezpečnosti - „Já nemám, co skrývat, já s žádnými tajnými daty nedělám.“
  - ▶ A používáte Facebook / Instagram / WhatsApp / Signal...?
  - ▶ Co by se stalo, pokud by se Vašeho účtu zmocnil někdo, u koho byste si to rozhodně nepřáli?
    - ▶ Zveřejnění posměšného statusu je jen to nejmenší.
- ▶ Kybernetická bezpečnost se týká každého uživatele Internetu.



# Základy

- ▶ Silná a unikátní hesla,
- ▶ šifrování,
- ▶ používání VPN,
- ▶ ...ale především rozum. 😊

Hesla 

# Heslo

- ▶ Klíč k Vaší online identitě
  - ▶ Znalostí hesla prokazují službě, že „já jsem já“ a že mi může zpřístupnit údaje, které jsou jen pro mě
- ▶ Kdo jej získá, může se za Vás vydávat
- ▶ Je zapotřebí si jej chránit „jako oko v hlavě“

CHRAŇTE A BRAŇTE SVOJE  
HESLO, JEST TO KLÍČ K VAŠÍ  
ELEKTRONICKÉ IDENTITĚ ...



# Silná hesla

- ▶ Mluví se o nich již od nepaměti
- ▶ Doporučená podoba se v průběhu času mění v souvislosti s běžně dostupným výkonem počítačů
- ▶ Osmiznaková hesla dnes již nejsou považována za bezpečná, minimum je dnes 12 znaků
  - ▶ Dobrá jsou tzv. frázová hesla, např.: „trhat.fialky.B00M.dynamitem“
  - ▶ Nejlepší jsou hesla typu \$kLKC{~A<BXh42:{, ty si lze ale jen těžce pamatovat
- ▶ Do každé služby by mělo být jiné (unikátní) heslo

HMM, ALE JAK SI VŠECHNA TA  
HESLA MÁM PAMATOVAT...?



# Správci hesel

- ▶ Programy, jež v šifrované podobě uchovávají Vaše hesla
  - ▶ Přistupujete k nim pomocí tzv. **master password**, jediného hesla, které si musíte pamatovat
- ▶ Umožňují používat do každé služby jiné (komplikované) heslo bez nutnosti si je všechny pamatovat
- ▶ Často umožňují i generování velmi silných hesel
- ▶ Správci hesel v prohlížečích nebývají nejspolehlivější
- ▶ Dobrý je **KeePass**, ten je ale celkem „old-school“ 😊
- ▶ Populární je také **LastPass**
- ▶ Dobrý správce hesel je open-source!



# Správci hesel

## Pro

- ▶ Do každé služby je jiné heslo
- ▶ Hesla mohou být velmi silná bez nutnosti pamatování
- ▶ Uchování dat v bezpečně zašifrovaném souboru

## Proti

- ▶ Dáváte „všechna vajíčka do jednoho košíku“ - kdo zjistí master password, ten má přístup ke **všem heslům!**
  - ▶ Do nejkritičtějších služeb (E-mail, Facebook, bankovníctví) si hesla stále noste v hlavě.
- ▶ Mírné snížení uživatelského komfortu - nutnost instalace dalšího SW a interakce s ním.



S HESLY BY TO BYLO VŠECHNO.  
TED ZAJISTÍME, ABY NÁM JE  
NIKDO NEODCIZIL.

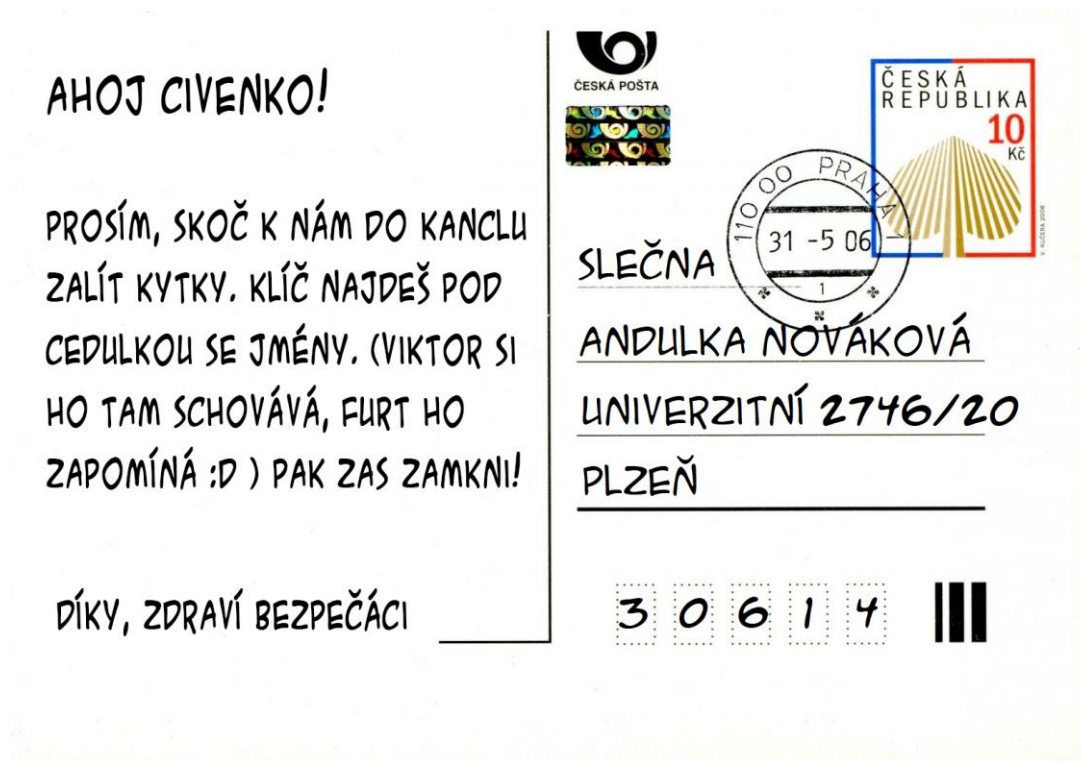


# Šifrování

„Dance like no one is watching. Encrypt like everyone is.“

# Šifrování

- ▶ Silné heslo je důležité, ale schováním do správce hesel jeho ochrana nekončí.
- ▶ Odesláním hesla přes nešifrovaný protokol jej prakticky dáváme k dispozici každému, kdo se k datům po cestě Internetem dostane.
- ▶ Poslali byste snad takovou pohlednici...?



# Šifrování

- ▶ = proces utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí. [Wiki]
- ▶ Dlouhá historie, vyvíjeno mj. zejména pro armádní účely
- ▶ Nejjednodušší je asi tzv. Caesarova šifra
  - ▶ *Klíč najdeš pod cedulkou se jmény. => Pqng seohix uth gihzqptz xi orisc.*
- ▶ V počítačích se dnes nejčastěji využívají šifrovací algoritmy **AES** a **RSA**, oba jsou využity při webové komunikaci přes **HTTPS**. (*HTTP over SSL*)

# Šifrování



http://login.seznam.cz

**SEZNAM.CZ**

## Přihlášení do Emailu

Jeden účet pro všechno od Seznamu

Seznam.cz Čeština

E-mailová adresa @seznam.cz

Heslo

Nemůžete se přihlásit?

**Přihlásit se**

Pokud ještě nemáte účet, tady si ho [vytvoříte](#).

Zabezpečte si lépe své [přihlašování](#).



https://login.seznam.cz

**SEZNAM.CZ**

## Přihlášení do Emailu

Jeden účet pro všechno od Seznamu

Seznam.cz Čeština

E-mailová adresa @seznam.cz

Heslo

Nemůžete se přihlásit?

**Přihlásit se**

Pokud ještě nemáte účet, tady si ho [vytvoříte](#).

Zabezpečte si lépe své [přihlašování](#).

# Šifrování



http://login.seznam.cz

- > Hypertext Transfer Protocol
- ▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  - > Form item: "username" = "pepik1997"
  - > Form item: "password" = "tajneheslo"
  - > Form item: "logon" = "Login"

```
0180 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Referer: http://10.109.25.2/logon/LogonRpm.htm Accept-Encoding: gzip, deflate Accept-Language: cs-CZ,cs;q=0.9 user-name=pepik1997&password=tajneheslo&logon=Login
```



https://login.seznam.cz

- > Transmission Control Protocol, Src Port: 58489, Dst Port: 443, Seq: 698, Ack: 5098, Len
- ▼ Transport Layer Security
  - ▼ TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
    - Opaque Type: Application Data (23)
    - Version: TLS 1.2 (0x0303)
    - Length: 931
    - Encrypted Application Data: d12dac9da1e4be6e564ed4972b760a72ecb94b3e9440a8fd0004e[Application Data Protocol: http-over-tls]

```
0020 4c 37 e4 79 01 bb 99 80 85 22 b1 6a 68 59 50 18 L7y.....".jhYP  
0030 04 02 32 ab 00 00 17 03 03 03 a3 d1 2d ac 9d a1 ..2.....  
0040 e4 be 6e 56 4e d4 97 2b 76 0a 72 ec b9 4b 3e 94 ...nVN++v...K>  
0050 40 a8 fd 00 04 e0 4d a8 34 b7 41 7c fd 48 8b 14 @.....M.4.A|.H.  
0060 7d 93 d5 d4 c0 2c 63 dc c9 91 ed 7d 82 48 08 46 }.....c....}.H.F  
0070 a7 a2 c1 9a b5 17 a5 42 b4 b1 92 68 4d 48 05 79 .....B...hMH.y  
0080 47 40 c8 a5 a0 2a 38 c9 99 89 5a 9d c6 60 9c 1a G@...*8...Z...  
0090 8f 7c 0a 49 ad 9c 41 fc 6e 10 4d d0 66 17 f0 9c .|.I..A..n.M.f...  
00a0 39 6a 94 03 4b ca 2d 0f d6 dd 8b c7 b8 02 59 db 9j...K...Y...  
00b0 84 e8 fd 0d 96 63 b5 ff ef 38 6a ad 57 52 e6 1f .....c...8j.WR...  
00c0 e7 e6 cc 4f 7a 28 a7 c5 fe c2 ed 22 f7 c2 af 72 ...Oz(...)...r  
00d0 43 46 09 19 10 5e 27 94 34 b6 6a 31 de 43 bf 60 CF...^'.4.j1.C`  
00e0 f1 58 bf 13 f0 1b 87 30 3c 77 91 2c f0 6c 19 a4 .X.....0 <w.,.1...  
00f0 0a f3 7e 62 db 34 46 a0 f8 04 43 92 dd 18 65 67 ...~b.4F...C...eg  
0100 6b ec fc ff b9 53 50 8e b8 85 6b 09 2f f3 be a3 k....SP...k/...  
0110 a8 be b7 e0 2e 96 12 35 07 97 88 31 af b1 80 d0 .....5...1....  
0120 4e 50 8b 2c 37 79 41 3d ef 5d 62 08 40 7e 3d a0 NP.,7yA=.]b@v==  
0130 e9 7d bb 48 be 8e 3b 73 db 28 c3 c5 78 10 97 08 .}H.;s.(.x...  
0140 8b 0b 03 d7 00 d2 0a b0 b8 4b 0a 22 a9 c2 d6 bd .....K...  
0150 5c 0f 5f e5 aa 3f f9 7c 09 ee 87 b5 b0 12 b3 88 \_...?|.....
```

# Co HTTPS zaručuje a co nikoliv?

- ▶ HTTPS zaručuje, že data budou po síti přenesena v šifrované podobě.
- ▶ HTTPS nezaručuje, že stránka, na kterou data zadáváte, není podvodná.



www.seznam.cz



www.seznam.cz.blogger.com/dG90byBqZSBwb2R2b2Q=

- ▶ Certifikát pro používání HTTPS si dnes může nechat vystavit každý.

ZÁMEČEK TAM MAJÍ. TEĎ TOMU  
VŠICHNI BUDOU VĚŘIT. MUHAHA



# Šifrování

## ▶ NEIGNOROVAT:



Vaše připojení není soukromé

Útočníci se mohou pokusit ukrást vaše údaje z **www.seznam.cz** (např. hesla, zprávy či údaje z kreditních karet).

NET::ERR\_CERT\_AUTHORITY\_INVALID

[Zpět do bezpečí](#)

### ▼ Help me understand

Server nedokázal prokázat, že patří doméně **www.seznam.cz**. Operační systém vašeho počítače nedůvěřuje jeho bezpečnostnímu certifikátu. Může to být způsobeno nesprávnou konfigurací nebo tím, že vaše připojení zachytává útočník.

[Pokračovat na www.seznam.cz \(není bezpečné\)](#)



Vaše připojení není soukromé

Útočníci se mohou pokusit odcizit vaše údaje na webu **www.seznam.cz** (například hesla, zprávy nebo informace o platebních kartách). [Další informace](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

[Rozšířená nastavení](#)

[Zpět na bezpečnější stránku](#)

# Šifrování e-mailu

- ▶ Používáte-li e-mailového klienta, věnujte pozornost zabezpečení jeho komunikace se serverem.
- ▶ Drtivá většina běžně používaných e-mailových serverů dnes nabízí šifrování přes SSL - tedy stejnou metodou, jako u HTTPS.
- ▶ **V případě nešifrování je riziko krádeže hesla násobně vyšší, než u procházení webu** - e-mailový klient provádí pravidelnou synchronizaci, při níž pokaždé pošle heslo.



# Jak to nastavit?

- ▶ Obecně, vyžadujte protokoly, co používají SSL.
- ▶ Pro příjem pošty - ~~protokol IMAP na portu 143~~ => protokol IMAPS na portu 993  
...nebo...
- ▶ Pro příjem pošty - ~~protokol POP3 na portu 110~~ => protokol POP3S na portu 995
- ▶ Pro odesílání pošty - ~~protokol SMTP na portu 25~~ => protokol SMTPS na portu 465
- ▶ STARTTLS se obecně NEDOPORUČUJE.

# Kde to nastavit?

- ▶ MS Outlook: Nastavení účtu -> Správa profilů -> E-mailové účty -> *Váš účet* -> Další nastavení -> Upřesnit
- ▶ Mozilla Thunderbird: Pravé tlačítko na Vaši schránku -> Nastavení -> Nastavení serveru / Server pro odchozí poštu (SMTP)

Nastavení serveru

Typ serveru: Poštovní server (IMAP)

Adresa serveru:  Port:  Výchozí: 993

Uživatelské jméno:

**Nastavení zabezpečení**

Zabezpečení spojení:

Způsob autentizace:

**Nastavení serveru**

Po spuštění zkontrolovat nové zprávy

Kontrolovat nové zprávy každých  minut

Povolit okamžité upozornění pro nové zprávy

Při odstranění zprávy:

Přesunout zprávu do této složky:

Označit zprávu jako smazanou

Okamžitě zprávu smazat (D)

Nastavení internetového e-mailu

Obecné Server pro odchozí poštu **Upřesnit**

Čísla portů serveru

Server pro příchozí poštu (IMAP):  Použít výchozí

Použít tento typ šifrovaného připojení:

Server pro odchozí poštu (SMTP):

Použít tento typ šifrovaného připojení:

Časové limity serveru

Krátký  Dlouhý 1 minuta

Složky

Cesta ke kořenové složce:

Odeslané položky

Neukládat kopie odeslaných položek

Odstraněné položky

Označit položky pro odstranění, ale nepřesunovat je automaticky

Položky označené pro odstranění se trvale odstraní při vyprázdnění položek v poštovní schránce.

Vyprázdnit položky při přepínání složek v online režimu

OK Zrušit

VPN

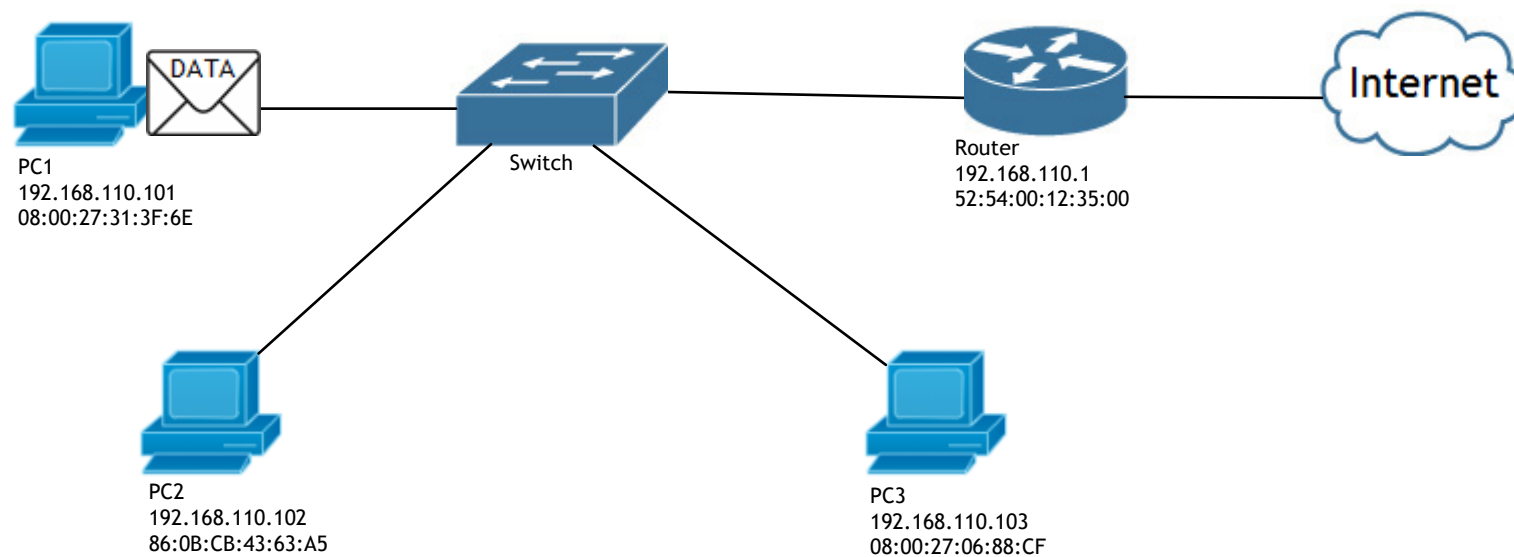


# VPN

- ▶ V dnešní době je již většina síťové komunikace šifrovaná
- ▶ Přesto může případný útočník v síti zjistit podstatné množství informací:
  - ▶ IP adresy, se kterými Vaše zařízení komunikovalo, včetně časových značek a množství přenesených dat,
  - ▶ domény, které jste si překládali,
  - ▶ další drobná data, která šla po nešifrovaných protokolech.
- ▶ V důvěryhodných sítích to nemusí být tak velký problém, ve veřejných sítích je to ale podstatná věc.

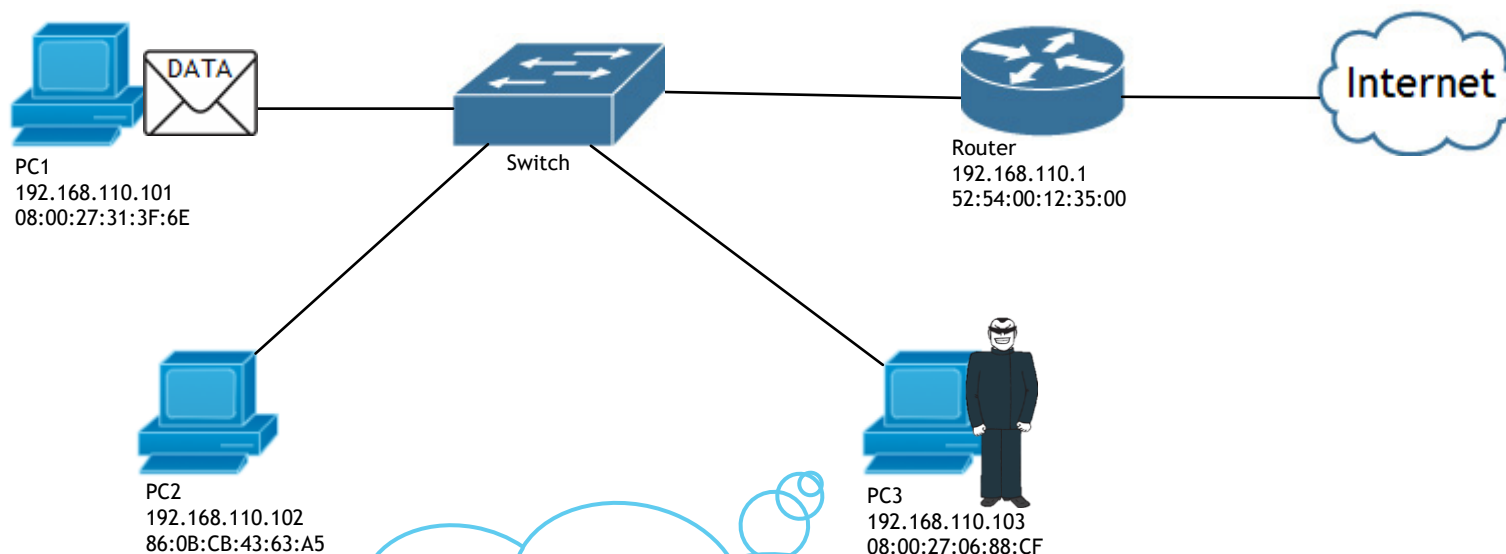
# VPN

- ▶ Tok dat bez použití VPN



# VPN

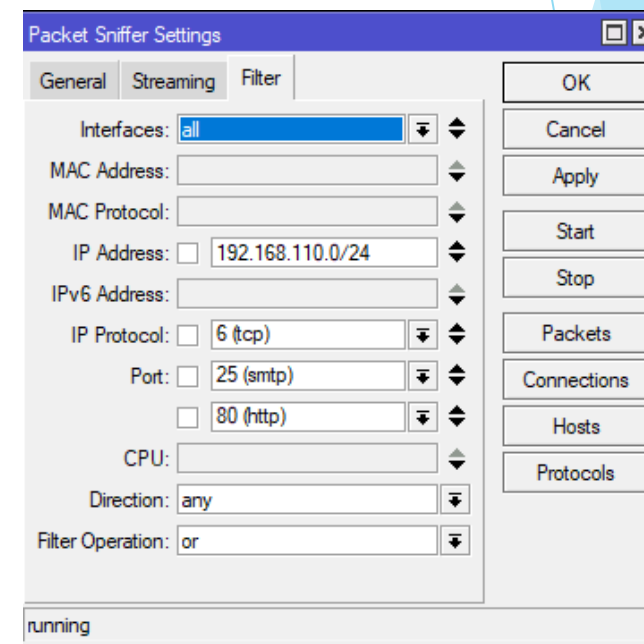
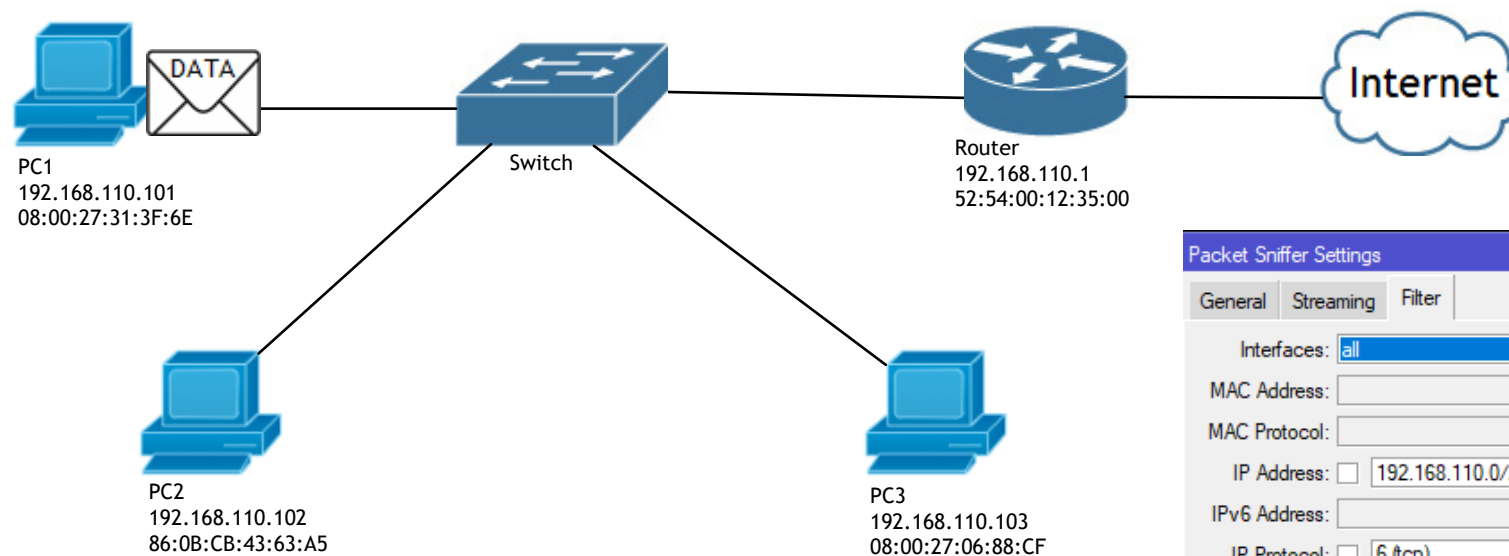
- ▶ Tok dat bez použití VPN



Ahá! Tak uživatel PC1 si tu překládal DNS [www.zcu.cz](http://www.zcu.cz) a pak přistupoval na jejich IP přes port 443 - takže web. Už vím, jak mu líp zacílím příští phishing. Muhaha.

# VPN

- ▶ Tok dat bez použití VPN



# Co s tím?

- ▶ Řešením je použití VPN.
- ▶ VPN (= Virtual private network) je technologie k propojování vzdálených sítí.
- ▶ Umožňuje Vám vytvořit si šifrovaný tunel mezi Vaším počítačem a jakoukoli vzdálenou sítí (přes její VPN koncentrátor) a všechna data posílat přes něj.
- ▶ Případný útočník tak uvidí pouze komunikaci dvou IP adres a změt' zašifrovaných dat.

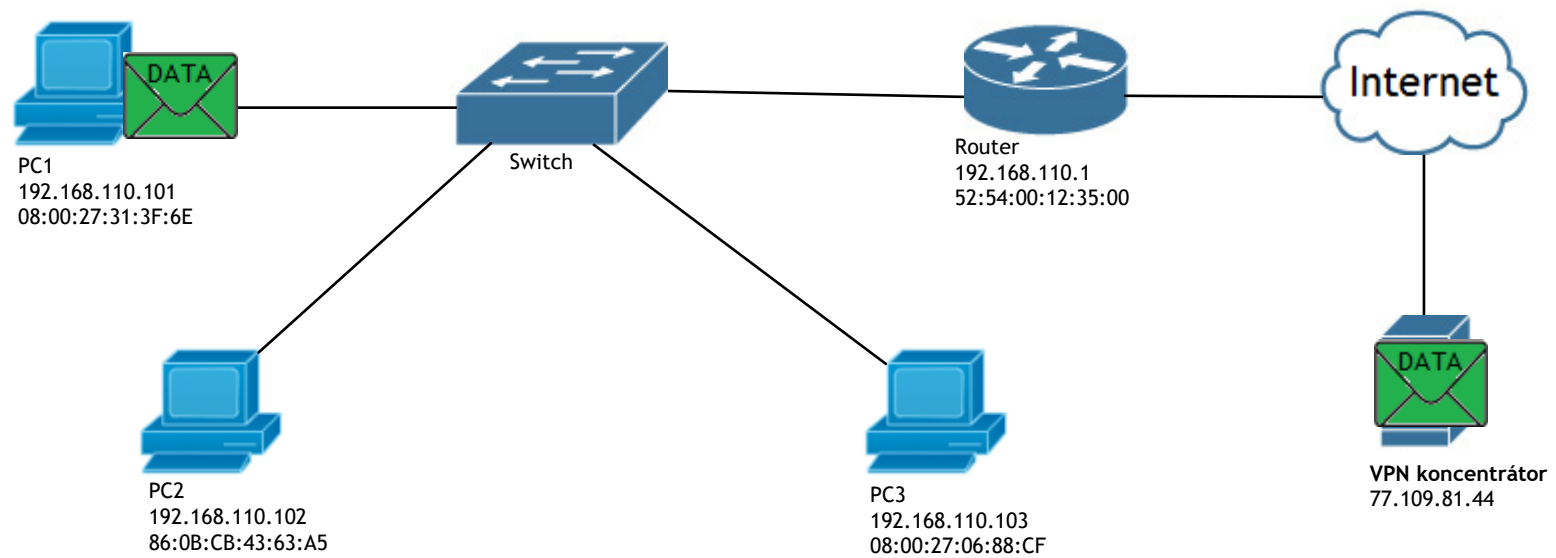
```
> Internet Protocol Version 4, Src: 192.168.0.100, Dst: 81.201.45.168
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
  UDP Encapsulation of IPsec Packets
    Encapsulating Security Payload
      ESP SPI: 0x02ea63ba (48915386)
      ESP Sequence: 469
```

---

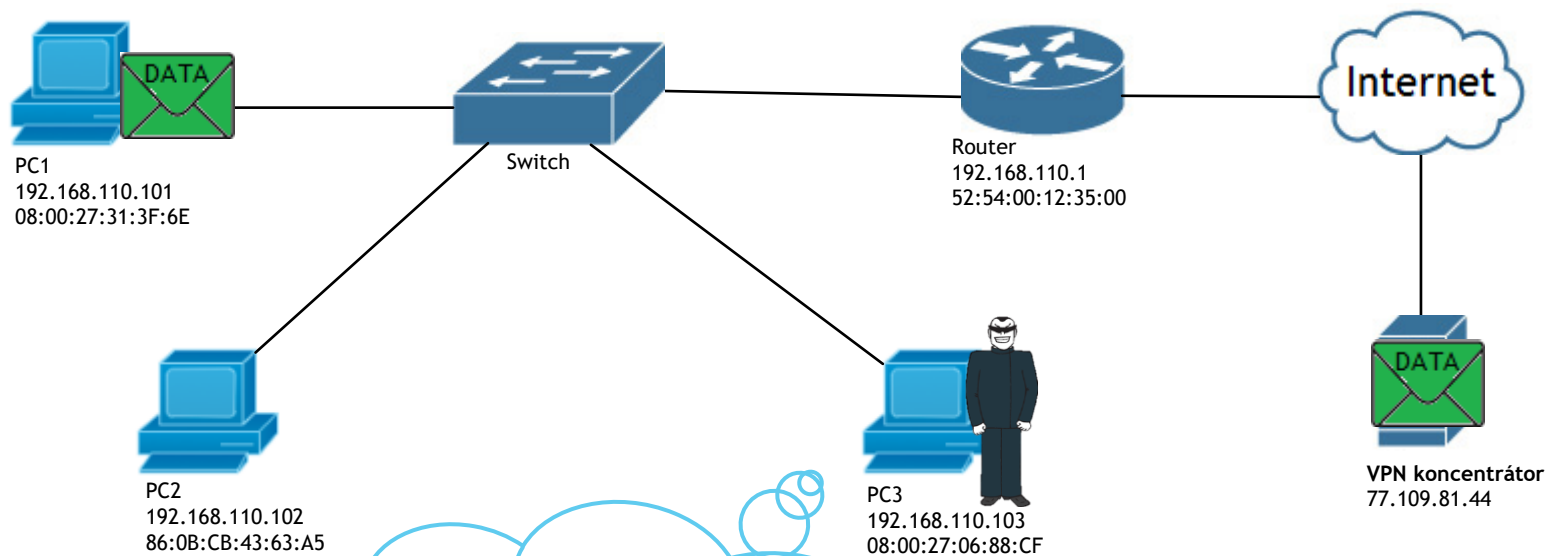
```
0140 a5 a3 83 cc 09 ec 9c 85 d0 e3 5c 20 07 6b 91 f5 ..... \ .k..
0150 de 83 44 2d bf 32 c1 f3 75 9b 9c e6 ff 5c 56 ff ..D-2.. u....\V.
0160 70 bb af 36 38 b2 e0 a3 1b 17 61 cd 17 2b 3e b7 p..68... ..a..+>
0170 a7 28 0d 34 6d d2 d7 66 28 81 57 80 df 52 6d e1 (.4m..f (.W..Rm.
0180 df 2d af 8e 81 ac 23 f8 cb 4c 20 e7 f6 be b6 94 .....#..L.....
0190 2c af 91 c8 92 8f ab 22 45 70 69 e8 bd b0 0b 86 ,....." Epi.....
01a0 27 f0 c8 7f 54 46 e4 da 30 66 ab 99 99 c6 a9 29 '...TF.. 0f.....)
01b0 74 68 aa 3b 67 cb 80 60 40 c7 33 91 07 62 fa 08 th;g.. @.3..b..
01c0 6a ee a3 b5 51 7f ba a4 3d c9 a0 77 63 aa c0 3c j..0... =..wc<
```



# VPN



# VPN



...,#.l.^....Axj9..D..s.....  
0...0...U.....Z..h..]&Rjh0  
...U.#..0...N"T...n.....90...U.  
.....0...U.%..0...+.....+....  
...0...U.. ...WTF?!

# Zřízení VPN

- ▶ VPN nabízí mnoho poskytovatelů (NordVPN, TunnelBear, ExpressVPN, ...)
  - ▶ Většina z nich je ale placená, resp. jejich neplacené programy (pokud existují) jsou často nepoužitelné
- ▶ Pokud máte vlastní veřejnou IP a ten správný router, můžete si VPN koncentrátor zřídit sami doma.
  - ▶ Některé dražší routery Asus, nebo všechny Mikrotik
  - ▶ Základní účely plní, z podstaty věci však nenabídne vše, co komerční VPN

# Komerční vs. domácí VPN

## Komerční VPN

- 👍 Anonymizace v rámci místní sítě
- 👍 Anonymizace v Internetu
- 👍 Obvykle dobré šifrování
- 👎 Platí se za ni


## Domácí VPN

- 👍 Anonymizace v rámci místní sítě
- 👍 Je zdarma
- ± Může mít dobré šifrování
- 👎 Anonymizace v Internetu schází
  - Přípojka, přes níž data posíláte, je u Vašeho ISP psána na Vaše jméno

# Univerzitní VPN

- ▶ Specifikací podobná domácí VPN
- ▶ Potřebujete-li VPN jen na změnu IP (např. z důvodu geologických restrikcí českých služeb při cestě do zahraničí) a nechce se Vám za ni platit, je univerzitní VPN dobré řešení.
- ▶ <https://vpn.zcu.cz>

**Služba ZČU VPN Orion**



Orion login:

Heslo (password):

[Návody pro připojení prostřednictvím služby VPN Orion](#)

**Informace ke službě VPN Orion**  
Prostřednictvím služby VPN Orion získáte přístup do vnitřní sítě ZČU. Po přihlášení bude automaticky nainstalován program *Cisco AnyConnect Secure Mobility Client*, který vytvoří bezpečné šifrované spojení mezi vaším počítačem a VPN koncentrátorem umístěným v síti WEBnet.

Po připojení vám bude dynamicky přidělena IP adresa z rozsahu univerzity.

Pro přihlášení použijte stejné uživatelské jméno a heslo, jaké máte v distribuovaném prostředí ZČU Orion.

# Děkuji za pozornost, prostor pro dotazy!

Viktor Ferus - WEBnet Incident Response Team

[ferusvi@civ.zcu.cz](mailto:ferusvi@civ.zcu.cz)

[www.viktor-ferus.cz](http://www.viktor-ferus.cz)

<https://www.youtube.com/nokia6085ful>

Centrum Informatizace a výpočetní techniky, Západočeská univerzita v Plzni