STŘEDNÍ PRŮMYSLOVÁ ŠKOLA
TRUTNOV, ŠKOLNÍ 101

CENTRUM ODBORNÉHO VZDĚLÁVÁNÍ
v elektrotechnice a ICT

Bezpečnost Internetu

JE INTERNET BEZPEČNÝ?
A CO AUTO, JE BEZPEČNÉ?

Základem bezpečné jízdy autem je:

- Mít bezpečné auto:
  - Aktivní bezpečnost (jízdní asistenti)
  - Pasivní bezpečnost
- Dodržovat pravidla silničního provozu
- Přizpůsobit jízdu stavu vozovky a provozu
- Předvídat možné situace

„Nemůže se mi nic stát?“

Pokud ale:

- Auto nesplňuje dnešní požadavky na aktivní bezpečnost – nemá ABS, ESP a jiné asistenty
- Ani požadavky na pasivní bezpečnost – špatné brzdy, nemá airbagy, korozí narušená konstrukce
- Řidič si neláme hlavu s dodržováním předpisů
- Řidič neřeší aktuální situaci – nepřemýšlí

Havárie je podstatně pravděpodobnější.

A co komunikace na Internetu?

Pokud má uživatel vhodné vybavení (zabezpečený počítač) a dodržuje určitá pravidla, tak je i komunikace na Internetu poměrně bezpečná.

Bezpečná komunikace

„Oheň je dobrý sluha, ale zlý pán.“

Stejně tak auto nebo internetová komunikace, pokud jsou správně používané, jsou relativně bezpečné a bez nich by v dnešní době bylo těžké se obejít.

Nebezpečí z Internetu:

- Zavirování počítače
- Ztráta dat
- Zcizení informací
- Finanční ztráta

Jak zabezpečit počítač:

- Pravidelně aktualizovat operační systém (i další programy)
- Používat antivirový program a aktualizovat ho
- Používat správně nastavený firewall
- Pracovat na běžný uživatelský účet, ne jako správce (administrator, UAC)

Antivir

- Je to program, který monitoruje aktivity, probíhající v počítači.
- Pokud zjistí podezřelý soubor nebo chování nějakého programu tak zablokuje jejich použití nebo další činnost.

Jak se projevuje zavirovaný počítač?

- Podstatně se zpomalí
- Některé programy najednou správně nefungují
- Občas se „sekne“ nebo se náhodně restartuje
- Občas se nějaká data ztratí nebo jsou poškozená
- Počítač se stává zdrojem virové nákazy pro ostatní (většinou ty, se kterými komunikuji)

Další funkce virů:

- Rozesílá zavirované zprávy
- Umožňuje útočníkovi převzít kontrolu nad počítačem
- Využije napadený počítač pro útoky (DoS, DDoS)
- Využije napadený počítač pro rozesílání spamu
- Zjišťuje a odesílá přístupová jména a hesla pro různé služby (třeba Facebook, E-mail, internet banking, …)

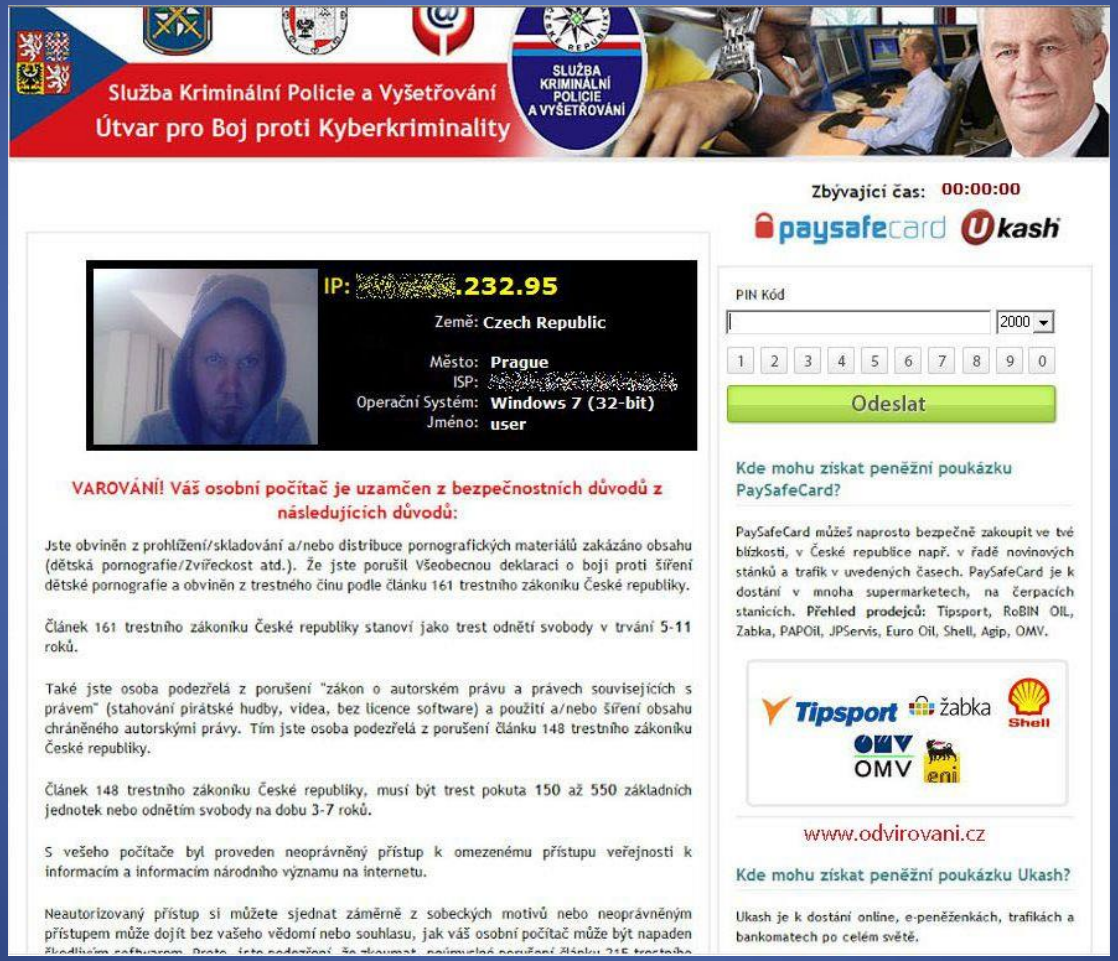
Co je to firewall

- Je to program, který monitoruje data, která přichází do počítače nebo z něj odchází a zjišťuje, zda se nejedná o pokus proniknutí do počítače
- Ve všech moderních operačních systémech je již zabudován a standardně zapnut
- Bývá součástí i antivirových programů (jako náhrada za systémový firewall)
- Je vhodné zapnout firewall i na rozhraní vnitřní (domácí, školní, firemní) a veřejné sítě (Internet)

Přístupová práva

- Většina útoků může využít credit (oprávnění) uživatele, který komunikaci s útočníkem vyvolal.
- Pokud pracuji jako běžný uživatel, mám jen oprávnění pro práci s programy, nemohu měnit součásti systému, systémová nastavení nebo instalovat programy.
- Proto se virus nemůže nainstalovat a škodit.

Policejní virus



Jak může dojít k zavirování počítače

- Instalace programu s virem
- Otevření zavirované přílohy e-mailu
- Spuštění viru odkazem z e-mailu nebo webové stránky

Jak předcházet zavirování počítače:

- Mít aktualizovaný a správně nastavený operační systém, antivir, firewall a případné další programy.
- Pracovat na běžný účet (bez práv administrátora).
- Instalovat jen nezbytné programy, z originálních a prověřených zdrojů (oficiální store).
- Zodpovědné chování uživatele

Chování při komunikaci na Internetu

- Neotevírat podezřelé e-maily a zejména jejich přílohy
- Nereagovat na nabídky instalací programů a nástrojů, které se objevují při procházení webových stránek
- Nezadávat osobní informace (zejména čísla účtů nebo kreditních karet)
- Vyhnout se nebezpečným stránkám - různé torenty, stahování cracků a nelegálního software, pornografie, … (nebo být extrémně opatrný)

Chování při komunikaci na Internetu

- Používat silná hesla (měnit je)
- Pro různé systémy používat různá hesla
- Na „veřejných“ počítačích neukládat zadávaná hesla, používat „privátní“ (anonymní) mód prohlížeče (neukládá historii, cookies)

Možné zneužití Internetu

- Kybergrooming
- Kyberšikana
- Krádež identity
- Počítačový stalking
- Zneužití webkamery
- Závislost na Internetu
- Sexting
- Viry
- Kyberterorismus

Kybergooming

- Jedná se o zmanipulování jiného uživatele za účelem jeho zneužití – typický příklad „Jsem mladá krásná holka, nechceš se sejít v soukromí?“
- Obrana – nevěřit všemu co mi někdo na Internetu tvrdí, nezveřejňovat příliš osobní informace.

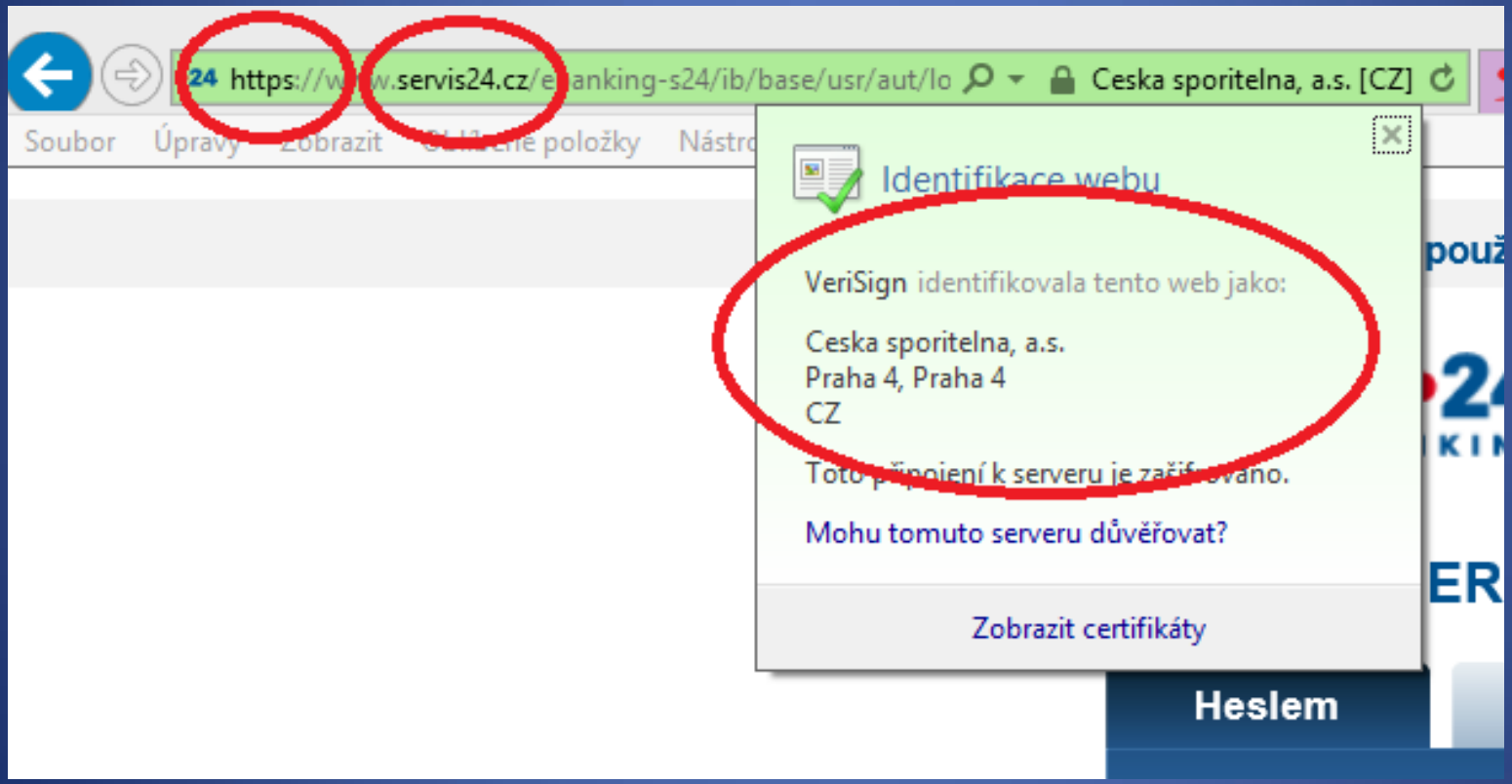
Kyberšikana

- Zneužití počítačových a mobilních komunikací k šikanování, vydírání a ubližování
- Obranou je opatrné zveřejňování osobních informací, v případě, že se stanete terčem kyberšikany využijte „linky důvěry“.

Krádež identity

- Vylákání nebo zcizení přístupových údajů do různých systémů, zejména do bankovních systémů.
- Obrana – nikdy nesdělovat tyto údaje do „neprověřených“ webových stránek. Pro placení kreditní kartou na Internetu používat jen prověřené systémy (např. PayPal)

Jak identifikovat webovou stránku



Počítačový stalking

- Systematické „obtěžování“ prostřednictvím ICT (počítač nebo mobilní telefon).
- Obrana – ukončit komunikaci, případně uložit komunikaci jako důkaz pro případné trestní řízení.

Zneužití webkamery

- Při videokonferenci může druhá strana nahrávat video, které potom zneužije, útočník může na Vašem zavirovaném počítači spustit videokameru i bez Vašeho vědomí!
- Obrana – zvažte, co vše při videokomunikaci ukazujete na kameru a s kým komunikujete.

Závislost na Internetu

- Je stále rozšířenější, obdobná jako jiné závislosti (hrací automaty, kouření, alkohol, drogy). Uživatel, který tuto závislost má, tak bez Internetu (zejména online komunikace) trpí abstinenčními příznaky
- Obrana – snažit se využívat jiné aktivity pro trávení volného času – zejména sport, jiné koníčky (modelářství, domácí zvíře, cestování, geocaching, …)

Sexting

- Posílání erotických (i odvážnějších) textů, obrázků a videí prostřednictvím Internetu (zejména sociálních sítí) nebo mobilním telefonem (SMS, MMS). Jednou vložené fotky (videa) do Internetu již autor těžko může beze stopy vymazat (neví, kolik lidí si je již stáhlo) a mohou být kdykoli (i po letech) zneužité.
- Obrana – neposílat intimní fotky a videa ani nejlepším přátelům.

Viry

- Bylo již vysvětleno.

Kyberterorismus

- Narušení počítačové komunikace a funkce počítačových řídících systémů (včetně vojenských)
- Obrana – důsledné dodržování bezpečnostních pravidel

Zdroje:

- Bezpečně online. *Bezpečně online* [online]. Národní centrum bezpečnějšího internetu [cit. 2016-01-10]. Dostupné z: http://www.bezpecne-online.cz
- …