

# 11 Pravidla pro zabezpečení PC

## Obsah hodiny



Obsahem této hodiny stanovení bezpečnostních pravidel a pravidel bezpečného chování na Internetu.

## Cíl hodiny



Po prostudování budete schopni:

- vyjmenovat a vysvětlit pravidla ochrany PC
- charakterizovat ohrožení PC ze strany internetu
- orientovat se v pravidlech bezpečného chování při používání internetu

## Klíčová slova



Firewall, Antivirus, Zápaly, Alternativní aplikace, Zálohování, Nebezpečí internetu

### 11.1 Jak ochránit počítač

#### Instalace a správná konfigurace firewallu a antiviru

Windows X, Windows Vista a Windows 7 už mají firewall v základní výbavě. Před instalací nového, je třeba tento původní inaktivovat – dva současně pracující firewally mohou vzájemně kolidovat a způsobovat vážné problémy systému.

Jako první se instaluje antivirus a až poté firewall.

#### Pravidelné aktualizace

Ani ty nejlepší firewally a antiviry na světě příliš neposlouží, pokud nebudou pravidelně aktualizovány. V nastavení programu nutno zvolit automatické aktualizování a kontrolu stavu programu.

Je třeba aktualizovat i samotný operační systém.

## **Včasná instalace „záplaty“ na používaný software!**

Existují viry, které používají tzv. bezpečnostní díry v operačních systémech a aplikacích. Pokud je taková chyba v programu zjištěna, jeho výrobce zpravidla připraví tzv. záplatu (patch), kterou lze na daný program aplikovat (nainstalovat), a tím chybu odstranit.

Tyto soubory jsou zpravidla k dispozici ke stažení na stránkách jednotlivých výrobců software. Je v zájmu uživatele sledovat aktuální situaci a nové záplaty co nejdříve aplikovat. Toto pravidlo platí zejména pro operační systémy.

## **Prověřování externích paměťových médií před připojením**

Přesto, že podle dostupných údajů asi 85 % zaznamenaných virových útoků přichází prostřednictvím e-mailu, nelze podceňovat ani „tradiční“ způsoby šíření škodlivých kódů. Stále častěji se objevují viry, které napadají flash disky a jejich prostřednictvím napadají PC.

## **Používání alternativních aplikací**

Vzhledem k tomu, že např. produkty společnosti Microsoft jsou oblíbeným terčem počítačových pirátů, je vhodné používat i ověřený software jiných značek. Příkladem takového SW jsou prohlížeče alternativní k Internet Exploreru.

## **Pravidelné zálohování**

Minimalizuje případné škody způsobené agresivním virem, nespolehlivým hardwarem apod. V porovnání s cenou ztracených dat je čas strávený zálohováním zcela zanedbatelný. Vytvořené zálohy je vhodné uložit na bezpečném místě (pro případ požáru či jiné živelné katastrofy).

## **„Čisté“ bootovací médium**

Může nastat případ, že na počítači, nelze spustit operační systém. Pro takový případ je vhodné mít k dispozici bootovací médium.

## **Kontrola nad počítačem a nad tím, kdo jej používá**

Riziko virové nákazy a ztráty dat vzrůstá úměrně s počtem lidí, kteří mají ke konkrétnímu počítači přístup. Stačí jediný nezodpovědný člověk, který přinese z domova zavirovaný flash disk, otevře e-mailovou přílohu s virem a je zle.

## **Ochrana přístupových údajů**

V současné době je důležitým prvkem ochrany počítače jeho zabezpečení pomocí vhodného bezpečnostního programu, který zajistí přístup pouze definovaným uživatelům, na základě autentizace a autorizace uživatele. Nejde pouze o zamezení virové nákazy, ale i o ochranu informací uchovaných v počítači.

## 11.2 Nebezpečí internetu

Je třeba si uvědomit, že informace stojí svou cenu. S připojením počítače na Internet vyvstává potřeba chránit se i proti nežádoucím průnikům ze sítě.

Je zejména nutná opatrnost při stahování souborů:

- z bezpečných stránek,
- přímo ze stránek výrobce.

Důležité je dodržování základních pravidel elektronické korespondence:

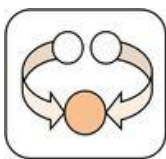
- Neodpovídat na zprávy, které se jeví z nějakého důvodu podezřelé.
- Neklikat na případné odkazy v podezřelých e-mailech.
- Neposílat osobní údaje někomu neznámému.
- Při rozesílání e-mailu více příjemcům vepisovat jednotlivé adresy do skryté kopie, aby se tak nedostaly do rukou ostatním příjemcům.
- Před otevřením přílohy e-mailu (ať už jde o jakýkoli typ souboru), provést kontrolu antimalwarem.

Nebezpečné je brouzdání po internetu jako uživatel administrátor; na internetu je vhodné být jen jako běžný uživatel. Pokud je vyžadováno vyplnění elektronické adresy například v diskusním fóru, je lépe si založit si raději novou schránku.

Nutná je zvýšená opatrnost při zasílání citlivých dat zejména z cizího počítače. Data posílaná elektronicky musí být dobře zabezpečena (zazipovat a opatřit heslem). Je vhodné vymazat veškeré stopy z prohlížeče.

Při online platebních operacích, je třeba při načtení dané stránky zkontrolovat, že jde o zabezpečené připojení (adresa začíná https a v pravé dolní části lišty prohlížeče se objeví zámeček) citlivých dat. Údaje jako číslo kreditní karty a podobně nepatří v žádném případě do e-mailu.

## Shrnutí kapitoly



Pro ochranu PC je třeba dodržovat následující bezpečnostní pravidla:

- Instalace a správná konfigurace firewallu a antivirového systému.
- Pravidelné aktualizace
- Včasná instalace „záplat“
- Kontrola externích paměťových médií, před připojením
- Používání ověřených alternativních aplikací
- Pravidelné zálohování
- Mít k dispozici „čisté“ bootovací médium
- Kontrola nad počítačem a nad tím, kdo jej používá
- Ochrana přístupových údajů

S připojením počítače na Internet vyvstává je nutno chránit se i proti nežádoucím průnikům ze sítě.

## Kontrolní otázky a úkoly



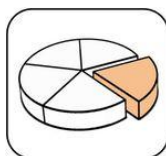
- 1) Jaká bezpečnostní pravidla je třeba dodržovat, abychom ochránili data v počítači.
- 2) Jaká jsou základní pravidla elektronické korespondence?
- 3) Jak se chránit na internetu?

## Otázky k zamyšlení



- 1) Jaká rizika pro bezpečnost dat hrozí ze strany Internetu?

## Použitá literatura a jiné zdroje:



- [1] Bezpečnost počítače. Itpoint.cz [online]. 31. března 2008 [cit. 2011-11-16]. Dostupné z WWW: <<http://www.itpoint.cz/zprava-itpoint.asp?id=1908&ico=48429627>>.