

## 17. Klasifikace bezpečnostních hrozeb pro počítače, možnosti ochrany PC.

S rozvojem informační a komunikační techniky na jednu stranu roste tempo a objem zpracovávaných informací, které pohánějí motor ekonomiky. Z druhé strany však s sebou tento rozvoj přináší nová ohrožení, kterým je nutno čelit. Komplexnost informačních a komunikačních systémů i celé IT infrastruktury, ve které se stále více prosazují virtualizační techniky, dosáhla bodu, kdy zajištění vysoké bezpečnosti a dostupnosti dat stojí stále více úsilí a prostředků. Podobně s nástupem nových technologií a způsobů komunikace vyrostla celá plejáda nových bezpečnostních rizik v oblasti počítačové bezpečnosti, jako jsou phishing, pharming či spyware, které připravily odborníkům v počítačové bezpečnosti nejednu horkou chvíli.

### Přehled soudobých hrozeb počítačové bezpečnosti

Název hrozby	Popis hrozby
Hacking	Hacking spočívá v úsilí o narušení soukromí uživatele počítačových sítí či poškození počítačových entit, jako jsou soubory, programy či webové stránky útočníkem (hackerem). Stupeň nebezpečnosti hackingu sahá od pouhého zneprůjemňování činnosti uživatelů až po nelegální aktivity, jako je krádež souboru dat.
Phishing	Phishing (někdy překládán do češtiny jako rhybaření) je podvodná technika používaná na internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) od obětí útoku. Jejím principem je rozesílání e-mailových zpráv, které se tváří jako oficiální žádost banky či jiné podobné instituce a vyzývají adresáta k zadání jeho údajů na odkazovanou stránku. Tato stránka může například napodobovat přihlašovací okno internetového bankovníctví a uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze.
Pharming	Pharming se snaží přesměrovat provoz legitimních webových stránek na stránky falešné, ale podobně vypadající, na kterých se pokusí vylákat od návštěvníka citlivé údaje jako například přihlašovací údaje do internetového bankovníctví. Jednou z metod pharmingu je napadení DNS serveru, který udržuje seznam internetových domén a příslušných DNS adres. Druhá metoda je založena na útoku proti jednotlivým počítačům. Počítače s operačními systémy Windows obsahují takzvaný soubor hosts, který funguje obdobně jako DNS server. Jestliže se útočníkovi podaří do tohoto souboru zapsat adresu své podvodné stránky, pak je efekt pro uživatele stejný jako v předchozím případě.
Malware	Malware je obecný termín pro škodlivý programový kód či software, který se bez vědomí uživatele snaží proniknout do počítačového systému a poškodit jej nebo z něj zcizit citlivé údaje. Malware zahrnuje širokou škálu škodlivých programových kódů zahrnující počítačové viry, červy, trojany, rootkity, spyware a další.
Spyware	Spyware je program, který využívá internetu k odeslání dat z počítače bez vědomí jeho uživatele. Někdy odesílá pouze data typu

Název hrozby	Popis hrozby
	přehled navštívených stránek či nainstalovaných programů za účelem zjištění potřeb nebo zájmů uživatele. Existuje ale i spyware odesílající hesla a čísla kreditních karet nebo spyware fungující jako zadní vrátka. Spyware se často šíří jako součást sharewaru. K druhům spywaru patří adware (obtěžující reklama), browser helper object (změna parametrů prohlížeče), hijacker (změna domovské stránky), dialer (přesměrování volání modemu), keystroke logger (odpozorování stisků tlačítek klávesnice) a remote administration (vzdálená správa počítače neautorizovanou osobou).
Počítačový virus	Virus je škodlivý počítačový kód, který se připojí k programu nebo k souboru a může poškodit software, hardware i soubory. Počítačový virus se šíří z počítače na počítač. Skutečný virus se však nebude rozšiřovat bez zásahu člověka. Někdo musí nastavit sdílení souboru nebo poslat e-mail, aby se virus rozšířil. Viry zpravidla infikují takzvané proveditelné soubory (nejčastěji s příponou .exe), jejichž spuštěním dojde k rozmnožení virového kódu.
Worm	Worm (červ) se šíří z počítače na počítač, ale na rozdíl od viru má možnost se šířit bez jakéhokoli přičinění člověka. Worm převezme kontrolu nad funkcemi v počítači, které mohou přenášet soubory nebo informace, a může se tak přenášet samostatně. Vysokým nebezpečím červů je jejich schopnost replikace. Červ může například rozesílat kopie sebe sama všem členům e-mailového adresáře, jejichž počítače poté provedou to samé, což způsobí dominový efekt. Worm může neúměrně zatěžovat operační paměť nebo přenosovou kapacitu sítě a vést tak k zahlcení či zhroucení počítačového systému či sítě.
Trojan	Trojský kůň je počítačový program, který se jeví jako užitečný, ale ve skutečnosti působí škody. Trojští koně se šíří tím, že jsou uživatelé zlákáni k otevření programu, protože si myslí, že pochází z legitimního zdroje. Některé trojany jsou pouze obtěžující, jiné mohou vážně poškodit systém či vymazat důležitá data. Na rozdíl od virů a červů se samy nereprodukuje infikováním dalších souborů ani samy sebe nereplikují.
Rootkit	Rootkit je sada počítačových programů a technologií, pomocí kterých lze maskovat přítomnost zákeřného softwaru v počítači (například přítomnost virů, trojských koňů, spywaru a podobně). Rootkity umožňují skrývat běžící procesy, soubory a systémové údaje, takže pomáhají útočnickovi zůstat skrytý.
Spam	Spam je nevyžádané masově šířené sdělení (nejčastěji reklamní) šířené internetem. Původně se používalo především pro nevyžádané reklamní e-maily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace – např. diskuzní fóra, komentáře nebo instant messaging.

## Možnosti ochrany PC

Kroky ke zvýšení (internetové) bezpečnosti

Antivirová ochrana je kombinací vašeho jednání a softwarových prostředků, tohle je doporučený postup virové prevence.

### 1. Věnujte pozornost činnostem, které provádíte

- Pečlivě sledujte, jaké programy na svůj počítač instalujete. Programy pochybného původu od neznámých tvůrců mohou mít vedlejší škodlivé funkce.
- Při návštěvě nedůvěryhodných stránek nedovolte žádnou akci, pokud si nejste jisti její bezpečností.
- Pokud chcete přistupovat na stránky vyžadující platbu pomocí telefonátu na číslo se zvýšeným tarifem, pečlivě se ujistěte, že znáte veškeré podmínky takového přístupu.

### 2. Pravidelně aktualizujte operační systém

- Používáte-li operační systém Windows, využijte služby Active Update.

### 3. Používejte antivirový program

- Nainstalujte si antivirový software a pravidelně jej aktualizujte.
- Provádějte pravidelnou kontrolu souborů na disku antivirem (např. 1x týdně).
- Nastavte antivir tak, aby kontroloval příchozí poštu, Internet, případně další komunikační kanály.
- Nastavte průběžnou (rezidentní) ochranu antiviru a automatického antivirového testování pro dokumenty a software přidávaný do systému.

Antivirový program v širším slova smyslu je počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého software (malware). K zajištění této úlohy se používají dvě odlišné techniky:

- prohlížení souborů na lokálním disku, které má za cíl nalézt sekvenci odpovídající definici některého počítačového viru v databázi
- detekcí podezřelé aktivity nějakého počítačového programu, který může značit infekci. Tato technika zahrnuje analýzu zachytávaných dat, sledování aktivit na jednotlivých portech či jiné techniky.

Úspěšnost závisí na schopnostech antivirového programu a aktuálnosti databáze počítačových virů. Četnost aktualizace antivirových a antispamových programů se z řádu měsíců a let posunula do řádu hodin a minut. Boj za bezpečnost informací se rozhořel a válečná vřava na bojové linii už asi, bohužel, nikdy neutichne.

### 4. Používejte osobní firewall ke kontrole příchozí a odchozí komunikace do sítě Internet

- Nainstalujte si osobní firewall a pravidelně jej aktualizujte.
- Pomocí osobního firewallu povolte jen odchozí spojení z počítače, a to pouze důvěryhodným aplikacím.
- Zjednodušenou formu ochrany nabízejí i programy pro kontrolu dialer virů.

### 5. Zvažte následující kroky k zabezpečení elektronické pošty

- Pravidelně aktualizujte poštovního klienta za použití oprav od výrobce software
- Zabraňte poštovnímu programu otevírat další zprávy bezprostředně po přečtení předchozí. Doporučuje se i vypnutí náhledu nových zpráv: