# Počítačová infiltrace

**Počítačovou infiltrací** nazveme jakýkoliv **neoprávněný vstup do počítačového systému**. Jde o termín s velice širokým významem, proto se tato publikace omezí jen na některé typy. Výše uvedené typy lze označit i názvem **MALWARE** – MALicious softWARE, **škodlivý software**.

# Počítačový virus

Počítačový virus lze chápat ze dvou základních hledisek:

• **Hledisko uživatelské** - Počítačový virus je jednou z mnoha hrozeb bezpečnosti a integrity počítačových systémů.

• **Hledisko programátorské** - Počítačový virus je počítačový program, tj. sled instrukcí procesoru, který může **infikovat jiný počítačový program** takovým způsobem, že do něj **zkopíruje své tělo**, čímž se infikovaný program stává prostředkem pro další aktivaci viru. Počítačový virus je schopen vykonávat pouze to, k čemu jej programátor-tvůrce naprogramoval. Hlavní věcí, kterou se od běžných programů odlišuje a čím se stává pro veřejnost přitažlivým, je právě **schopnost replikovat své vlastní tělo**. Díky této skutečnosti se začíná počítačový virus svým chováním přibližovat viru biologickému.

Počítačový vir není nic jiného než **„pouhý“** **program**. Na rozdíl od většiny programů, které se snaží uživatelům zjednodušovat a ulehčovat práci, počítačový vir se snaží o opak – **zmást uživatele, způsobit nefunkčnost vybraných programů** a v tom nejhorším případě **smazat cenná data** nebo rovnou celý disk. Hlavní charakteristikou počítačového viru je však jeho snaha **se šířit**. Vytvářet další svoje kopie a šířit se jak mezi počítači, tak i případně v rámci jednoho PC. Virus musí sám sebe replikovat a provádět další svoji činnost. Pravé viry tvoří jen jednu z mnoha podkategorií spadajících pod pojem „**Malware**“ (**Malicious Software – zákeřný, škodlivý, …. Software**).

# Historie Počítačových virů

Samotná historie **začíná na přelomu 60. a 70. let.** V této době se na sálových počítačích pravidelně objevoval program nazývaný "**králík**". Tyto programy, **klonující sebe sama**, obsazovaly systémové prostředky a tak **klesala výkonnost systému**. Králík většinou nekopíroval své tělo ze systému do sytému, to byly hlavně lokální úkazy. Hlavní příčinou králíků byly chyby nebo žert systémového programátora. První incident, který může být nazýván jako epidemie "počítačový virus", se stal na systému Univac 1108. Vir nazvaný **Pervading Animal** přidával sám sebe na konec spustitelných souborů, tak jak to dělají tisíce moderních virů.

      V **první polovině 70. let** se pod operačním systémem Tenex objevil nově vytvořený vir **The Creeper**, který k šíření využíval globální počítačovou síť. Vir byl schopný přenášet své kopie přes modem a síť do vzdálených stanic. Na boj proti tomuto viru byl vytvořen první známý **antivirový program Reeper**.

# Důvod vzniku virů

Je několik důvodů vzniku virů:

* Vytvářejí je programátoři velkých softwarových firem, kteří byli propuštěni ze zaměstnání - Pomsta
* Vytvářejí je mladí programátoři, kteří si chtějí vyzkoušet své schopnosti.
* Viry vytvářejí programátoři antivirových firem – Účel prodeje Antiviru
* K rozesílání spamu

# Typy počítačových virů

Podle toho, jakým způsobem viry pracují a jak se projevují, je lze rozčlenit do několika základních skupin:

**Bootviry**

Jak již sám název kategorie virů napovídá, jedná se o viry, které m**ají spojitost se zaváděním systému** (bootováním). Vir napadne **bootsektor** (většinou 1. sektor na disku) nebo **partition tabulku** pevného disku či diskety. Při zavádění systému je pak pohodlně aktivován a převezme kontrolu nad funkcemi systému.

**Souborové viry**

**Souborové viry napadají pouze soubory**. Jedná se o kapitolu virů, které se projevují nejrozmanitějším způsobem. Podle toho se dále dělí:

1. **Přepisující vir** – přepíše část programu, který napadl vlastním kódem. Díky tomu je velmi nápadný, a proto nemá mnoho šancí se rozmnožit.
2. **Link vir** – „přilepí“ se (přilinkuje) k napadenému souboru, což umožní chod programu a zároveň činnost viru.
3. **Doprovodný vir** – zkopíruje napadený soubor do souboru se stejným jménem, ale typu COM, a k tomu se připojí (vzniknou dva soubory, kde COM je nakažený). Vir využívá vlastnosti OS MS-DOS, jenž nejprve spouští COM soubory.
4. **Vir přímé akce** – provede destrukční akci a tím skončí. Například smaže celý disk a tím „zabije“ sám sebe.
5. **Rezidentní vir** – načte se a drží v paměti a tím snadno napadne soubory, se kterými se pracuje.
6. **Stealth vir** – vir s touto vlastností se umí načíst do paměti a kontroluje činnost systému. Pokud antivirový program kontroluje zavirovaný soubor, pak mu vir s touto vlastností vrátí kód před infekcí. Pro antivirové programy, jež nejsou vybaveny anti-stealth kontrolou, je vir prakticky nezjistitelný.
7. **Polymorfní vir** – Pro každý napadený soubor se kóduje jinak a vytváří i jinou dekódovací funkci. Takový vir nemá v žádném okamžiku v žádném z napadených souborů stejnou sekvenci svého kódu.
8. **Metamorfní vir** – obsahuje funkci, která při kopírování sebe sama kompletně přepíše a vir tak vypadá úplně jinak. Tento mechanismus je poměrně složitý a celá replikační funkce zabírá až 90 procent kódu viru.
9. **Fast infektor** – šíří se extrémně rychle díky tornu, že napadá soubory při spuštění i při jakékoliv manipulaci s nimi. Snadno se rozšíří a tím na sebe upozorní.
10. **Slow infektor** – na rozdíl od předchozího se šíří velmi pomalu a opatrně.

**Makroviry**

**Makroviry** se objevily až s příchodem makrojazyků především v textových editorech a tabulkových procesorech. Zákeřnost makroviru spočívá vtom, že vir je přenášen a uložen v dokumentu.

## Trojský kůň a červ

Zde se nejedná přímo o druh viru, ale spíše o **metodu jeho šíření**. V běžném jazyce se ale ustálily i tyto pojmy jako typy virů.

**Trojský kůň (trojan horse)** je program, který se zdá být něčím jiným (užitečným, zajímavým), ale ve skutečnosti provádí škodlivou činnost. Například **se vydává** za spořič obrazovky a mezitím **maže soubory na disku**. Trojský kůň také **může umožňovat přístup k PC útočníkovi**. Ve své podstatě se obecně nejedná o virus, protože se **sám nešíří**.

**Červ (worm)** je **programový kód**, který se šíří sám **prostřednictvím počítačové sítě**. K tomuto účelu na rozdíl od klasických virů nemusí využívat souboru (respektive jich využívá odlišným způsobem). Po celé síti se šíří díky bezpečnostním nedostatkům a často ke svému šíření využije souboru. Celý soubor je ale pak možno považovat za červa.

# Jak se viry projevují

**Obtěžující**

Příznaky obtěžujících virů spočívají například ve **výpisech nesmyslných hlášení na obrazovku**, která se zpočátku mohou zdát humorná, ale pokud každých 5 minut počítač napíše, že je unavený, pak uživatel asi dlouho s nervy nevydrží. Viry mohou obtěžovat také **záměnou kláves na klávesnici**.

**Destrukční**

**Destrukční viry** vzbuzují určitý respekt již při vyslovení této kategorie. Základním úkolem takových virů je **zlikvidovat data**. Chytré viry pracují tak, že nezničí všechna data na disku, ale postupně zaměňují pouze určité byty nebo řetězce. Uživatel takový vir těžko odhalí a při dlouhodobém působení nakazí i záložní kopie. **Jednoduché viry zničí okamžitě po napadení například obsah disku a tím vlastně zničí samy sebe**.

**Ostatní**

Spousta virů nevykonává žádnou přímo destrukční činnost, ale **pouze se snaží dále a dále šířit**. I takové viry **mohou způsobovat problémy, obsazovat paměť, brzdit síťový provoz** a podobně.

Další viry mohou **rozesílat informace z vašeho počítače** na jiné, kde si je může autor viru přečíst, šířit se automatickým rozesíláním elektronickou poštou, nebo třeba šifrovat data na disku.

# Viry na internetu

## Malware

**Malicious Software** zahrnuje kromě **samotných virů spoustu dalších typů programů**, jejichž výskyt v počítači **je nežádoucí**. Podíváme se tedy na další pojmy a typy této počítačové „havěti“ se kterou se můžeme běžně setkat.

**Pod souhrnné označení malware se zahrnují**[**počítačové viry**](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus)**,**[**počítačové červy**](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_%C4%8Derv)**,**[**trojské koně**](https://cs.wikipedia.org/wiki/Trojsk%C3%BD_k%C5%AF%C5%88_(program))**,**[**spyware**](https://cs.wikipedia.org/wiki/Spyware) **a**[**adware**](https://cs.wikipedia.org/wiki/Adware)**.**

## Spyware

**Spyware je program, který využívá Internetu k odesílání dat z počítače** bez vědomí jeho uživatele. Narozdíl od backdooru jsou odcizovány pouze „statistická“ data jako přehled navštívených stránek či nainstalovaných programů. **Tato činnost bývá odůvodňována snahou zjistit potřeby nebo zájmy uživatele a tyto informace využít pro cílenou reklamu**. Nikdo však nedokáže zaručit, že informace nebo tato technologie nemůže být zneužita. Proto je spousta uživatelů rozhořčena samotnou existencí a **legálností spyware**. Důležitým poznatkem je, že **spyware se šíří společně s řadou sharewarových programů** a jejich autoři o této skutečnosti vědí.

## Adware

**Obvykle jde o produkt, který znepříjemňuje práci s PC reklamou**. Typickým příznakem jsou **„vyskakující“ pop-up reklamní okna během surfování**, společně s vnucováním stránek (např. výchozí stránka Internet Exploreru), o které nemá uživatel zájem. Část Adware je doprovázena tzv. **„EULA“** - End User License Agreement – licenčním ujednáním. Uživatel tak v řadě případů musí **souhlasit s instalací**. Adware může být součástí některých produktů. Ačkoliv nás reklama doprovází během celé činnosti s daným programem, **odměnou je větší množství funkcí, které nejsou v klasické free verzi** (bez reklamy) dostupné.

## 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.**

**E-mailové adresy do spamových databází jsou získávány mj. pomocí robotů**, které procházejí webové stránky a **sbírají e-mailové adresy** na nich uvedené. Také **registrací na některých serverech** s uvedením vaší adresy je možné přidat se na seznam pro spam. No a samozřejmě **viry na PC mohou odeslat seznam vašich kontaktů** nebo přímo odesílat spam z vaší adresy.

## Backdoor, Zombie, Botnets

**Některé viry** (červy) často jako svojí další činnost **instalují do PC tzv. Backdoor** (zadní vrátka), které **umožní k systému přístup útočníkovi**. Z takto nakaženého PC může být **vytvořena „zombie“** pod kontrolou autora viru. Sítě takových strojů se nazývají **botnets** a často jsou využívány k další nekalé činnosti jako je např. **odesílání spamu nebo provádění DDoS** (Distributed Denial of Service) útoků.

## Hoax

V počítačovém světě slovem HOAX nejčastěji označujeme **poplašnou zprávu**, která **varuje před neexistujícím nebezpečným virem.**

## Phishing

**Phishing je činnost, při které je rozesílán email uživatelům Internetu**, který **se tváři**, že byl odeslán z **legitimní organizace** (**většinou finanční, banky apod**.). Předmětem takového emailu **je získat osobni informace uživatele**, zejména pak **čísla platebních karet a jejich PIN** a následně jejich zneužití. Phishing email obsahuje často **odkaz na stránky s formulářem**, který uživatel v dobré víře vyplní a odešle. Odeslaná data vsak **nekonči u bankovního či finančního ústavu, ale v rukou tvůrce phishing** emailu.

# Způsob ochrany

Dokud byly počítače pouze samostatné stanice, existovalo hlavně nebezpečí virů a to zanesených z infikovaných médií. Jsou-li však počítače připojeny do počítačové sítě nebezpečí vzrůstá a s přístupem k internetu jsme prakticky stále v potenciálním ohrožení.

# Firewall

Jako obrana proti nebezpečí ze sítě existuje **firewall**. Hned na úvod je třeba říci, že **nenahrazuje antivirový program**, antispyware a další, ale v kombinaci nám dovolí mnohem lépe ochránit náš systém.

V počítačové terminologii se firewallem nazývá software či hardware (hardwarové firewally), **jehož funkcí je kontrolovat** (povolovat či zakazovat) **komunikaci v počítačové síti** na základě daných pravidel. Používá se na oddělování různých částí sítě (**nejčastěji odděluje nebezpečný internet od místní sítě**).

Mezi typické představitele paketových filtrů patří např. tzv. [**ACL**](https://cs.wikipedia.org/wiki/Access_control_list)**(Access Control Lists)** ve starších verzích operačního systému [IOS](https://cs.wikipedia.org/wiki/Cisco_IOS) na routerech spol. [Cisco Systems](https://cs.wikipedia.org/wiki/Cisco_Systems), popř. [JunOS](https://cs.wikipedia.org/wiki/Junos) spol. [Juniper Networks](https://cs.wikipedia.org/wiki/Juniper_Networks), starší varianty firewallu v [linuxovém](https://cs.wikipedia.org/wiki/Linux) jádře ([ipchains](https://cs.wikipedia.org/wiki/Ipchains)).

Přes hraniční firewall se zabezpečuje vnitřní síť (tzv. Bezpečnostní politika společnosti).

**Firewall** se zaměřuje pouze na hlavičku paketu (Zdrojovou MAC adresu; Cílovou MAC adresu; Zdrojovou IP adresu; Cílovou IP adresu; **Zdrojový a cílový Port**). Soustředí se na pravidla odchozích a příchozích portů. To znamená, že když k bráně dorazí paket s portem XXX a firewall nebude mít ve své tabulce povoleno přijímat pakety s portem XXX, paket rovnou zahazuje.

## Ochrana na Úrovni paketu

Paket označuje v [informatice](https://cs.wikipedia.org/wiki/Informatika) blok [dat](https://cs.wikipedia.org/wiki/Data) přenášený v [počítačových sítích](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5) založených na [přepojování paketů](https://cs.wikipedia.org/wiki/P%C5%99epojov%C3%A1n%C3%AD_paket%C5%AF), kde je možné přenášet data i při výpadcích některých spojů. Některé typy síťových spojů přenos paketů nepodporují (například tradiční telekomunikační linky typu bod-bod, [anglicky](https://cs.wikipedia.org/wiki/Angli%C4%8Dtina) point-to-point) a data se v nich přenášejí jako proud [bajtů](https://cs.wikipedia.org/wiki/Byte), znaků nebo [bitů](https://cs.wikipedia.org/wiki/Bit).

**Paket se skládá z 2 částí: Hlavička a Tělo (Tělo se někdy dělí na Tělíčko a patičku);**

**Hlavička obsahuje**: Zdrojovou MAC adresu; Cílovou MAC adresu; Zdrojovou IP adresu; Cílovou IP adresu; **Zdrojový a cílový Port;**

**Tělo obsahuje: Data**; Sekvenci dat;

**Patička obsahuje**: CRC (Kontrolní součet);

# Antiviry

**Proti virům je třeba se bránit**. V dnešní době si již nemůže být jistý žádný uživatel počítače, který datově komunikuje alespoň částečně se svým okolím. Kromě opatrnosti jsou **silným prostředkem proti virům antivirové programy**. Dokáží nejen najít vir, ale někdy i „**vyléčit**“ nakažený soubor tak, že po zásahu antivirového programu funguje správně a nemusí být celý smazán.

Na softwarovém poli působí poměrně velké množství antivirových programů. **Antivirový program by měl používat každý**, kdo je alespoň částečně nucen komunikovat prostřednictvím disket nebo jiného typu média s daty na jiných počítačích a kdo je propojen do sítě s jinými počítači. Antiviro**vou kontrolu by měl uživatel provádět v pravidelných intervalech.** Důležitá je také **aktualizace virové databáze** – načtení nově zjištěných virů do databáze antivirového programu je nutné proto, aby antivirový program byl schopen nové **viry identifikovat a odstranit**. Aktualizace se provádí většinou přes internet, může být však ještě realizována pomocí disket nebo CD. Virus bez aktuální virové databáze je většinou téměř k ničemu, protože nedokáže zachytit novější viry (které se také nejvíce šíří.)

Některé antivirové programy: **NOD32, Avast! AVG, Kaspersky AV, Norton AV, Windows Defender**

Při kontrole souboru antivirový program zjišťuje, zda se nějaká jeho část neshoduje s některým ze známých virů, které má zapsány v databázi. Pokud je nalezena shoda, má program tyto možnosti:

1. pokusit se opravit/vyléčit soubor odstraněním viru ze souboru (pokud je to technicky možné)
2. umístit soubor do karantény ([virus](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus) se dále nemůže šířit, protože ho nelze dále používat)
3. smazat infikovaný soubor (i s virem)

K dosažení trvalého úspěchu ve středním a dlouhém období vyžaduje virová databáze pravidelné aktualizace, které obsahují informace o nových virech. Pokud je antivirový program neaktualizovaný, představují viry přinejmenším stejné nebezpečí, jako kdyby antivir v počítači vůbec nebyl!

### Virové slovníky/databáze

Antivirový program fungující na platformě [databáze virů](https://cs.wikipedia.org/w/index.php?title=Slovn%C3%ADk_vir%C5%AF&action=edit&redlink=1) kontrolují soubory v momentě, kdy je operační systém počítače vytvoří, otevře, zavře nebo je zasílá/přijímá emailem. V takovém případě je virus možné zjistit ihned po přijmutí souboru. Nutno podotknout, že uživatel může naplánovat kontrolu celého systému (pravidelně, nebo na určitý čas). Lze tedy plánovat opakované kontroly všech/části souborů, které se na jednotlivých discích nacházejí. Velmi často je antivirová kontrola naplánována ihned po startu počítače.

Ačkoli lze při kontrole za pomoci virových databází virus spolehlivě zničit, tvůrci virů se vždy snaží být o krok napřed v psaní virových softwarů pomocí "oligomorfních", "polymorfních" a stále častěji "metamorfních" virů, které šifrují část sami sebe nebo jinak upravují vlastní kód jako metodu zamaskování před rozpoznáním virovými databázemi. Dalo by se říci, že jde o jakési dynamické mutace klasických virů, které není vždy jednoduché rozpoznat.

### 

### Nebezpečné chování

Metoda zjištění nebezpečného chování se oproti virovým databázím nesnaží najít známé viry, namísto toho sleduje chování všech programů. Pokud se takový program pokusí zapsat data do spustitelného programu, antivirus například označí toto nebezpečné chování a upozorní uživatele, který je antivirovým programem vyzván k výběru dalšího postupu.

**Antivirové programy se z pohledu paketu zabývají pouze tělem paketu a CRC.**

## Metoda - Skener

Základní typ programu, který zjišťuje přítomnost virů (v paměti i na disku) pomocí virových identifikačních řetězců. Identifikační řetězec je jednoznačně definovaná posloupnost znaků (bajtů) reprezentující daný virus.

## Metoda - Clean

Je-li úkolem skeneru virus najít, pak úkolem cleanu je nalezený virus odstranit. Odstranění viru, zejména souborového, je věcí velice choulostivou. Obecně platí zásada, že nejlepší odvirování souboru je jeho obnovení ze záložní kopie. Některé viry totiž nelze odstranit z důvodu jejich přepisovacího charakteru, jiné viry nelze odstranit se zárukou z důvodu jejich programových chyb apod. Velkým problémem jsou mutace virů, kdy virus může být, díky značné podobnosti s jiným virem, mylně identifikován a jeho odstranění je pak logicky nekorektní.

## Metoda - Kontrola integrity

Kontrola integrity (integrity checker, CRC checker) je založena na porovnávání aktuálního stavu důležitých programů a oblastí na disku s informacemi, které si o nich kontrolní program uložil při jejich příchodu do systému nebo při své instalaci. Pokud se do tímto způsobem chráněného počítače dostane vir, tak na sebe upozorní změnou některého z kontrolovaných objektů a je záhy detekován. Dají se tak spolehlivě zachytit i nové viry, o jejichž existenci nemají ponětí skenery, a které nemusí odhalit ani heuristická analýza.

## Metoda - Heuristická metoda analýzy

Virové identifikační řetězce selhávají v případech polymorfních virů, kdy má tělo viru při každé replikaci jinou podobu. Heuristika je jednou ze základních možností, jak lze polymorfní viry identifikovat. Navíc identifikační řetězce vyžadují častý „update“, nebo dokáží vyhledat pouze ty viry, které jsou obsaženy v databázi virových identifikačních řetězců.

## Metoda - Rezidentní štít

Možnost antivirové ochrany on-line. Rezidentní štít aktivním způsobem chrání počítač před virovou infiltrací v reálném čase. Nejčastěji jde o program typu skener, který provádí antivirovou kontrolu právě zpracovávaných dat. Rezidentní štít tak může zakázat zkopírování zavirovaných souborů z diskety na pevný disk či zakázat spuštění infikovaného programu apod.

# Antispyware

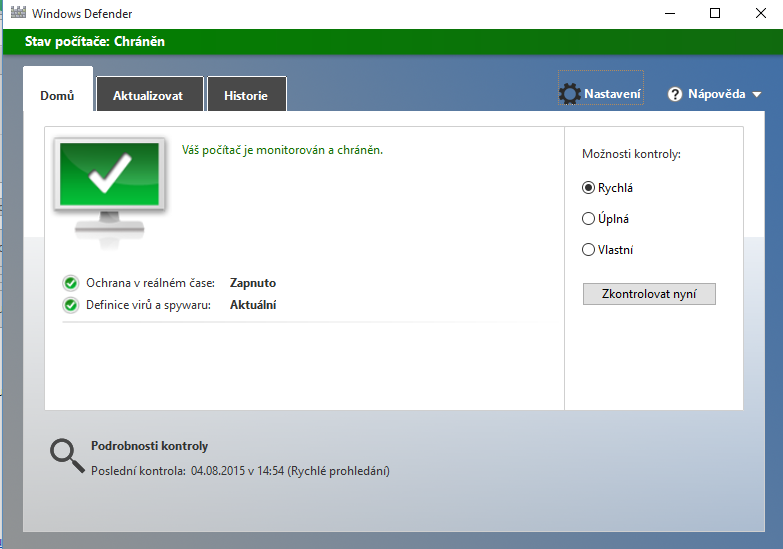
Na boj s viry, trojskými koňmi, červy atd. jsou antivirové programy, proti hackerům zase firewally a třetím doplňkem, který by v PC neměl chybět je **antispywarový nástroj**. Pomůže ochránit operační systém Windows před hrozbami typu spy kiware, adware apod. Tyto programové kódy skrytě pracují v PC a **odesílají důvěrné informace třetím osobám**. Mezi informace, které je schopen spyware zjistit a odeslat, patří jméno uživatele, IP adresa, seznam programů nainstalovaných na počítači, záznamy o aktivitě uživatelů a mnoho dalších dat.

# Jak se chránit

* Mějte nainstalovaný kvalitní antivirový systém
* Udržujte antivirový systém aktualizovaný (databázi program)
* Mějte v antivirovém systému zapnutou rezidentní ochranu
* Každou neznámou disketu, kterou vkládáte do svého počítače, nejprve otestujte antivirovým programem.
* Nepouštějte ke svému počítači nedůvěryhodnou cizí osobu
* Pravidelně zálohujte svá data.
* Buďte obezřetní. Většina virů se nějak projevuje. Ať je to delším zaváděním systému, podezřelým padáním programů, nebo jiným „neobvyklým“ chováním.
* Soubory stažené z internetu před spuštěním zkontrolujte antivirovým programem.
* Podezřelou či nevyžádanou e-mailovou poštu z internetu ani neotevírejte a ihned mažte.

# MS DEFENDER

Ve Windows 10 je **zabudovaný** Windows Defender, tedy antivirový program. Lze o něm říci, že na základní antivirovou ochranu plně postačí, ale pokročilejší věci od něj nečekejte. Stejně jako od něj nemůžete čekat, že by detekoval nějaké to adware, crapware a další zvířátka, na to pořád budete potřebovat něco víc.

Zapnutí a vypnutí Defenderu najdete v *Nastavení* -> *Aktualizace a zabezpečení* -> *Windows Defender*. Můžete tam vypnout **ochranu v reálném čase**, **cloudovou ochranu** (posílání informací do Microsoftího cloudu a čerpání informací z něj) a **Odeslání ukázkového souboru** (odeslání nalezeného malware, viru). Můžete zde nastavit i **Vyloučení,** kde určíte soubory/složky/typy souborů/procesy, které nemá Defender kontrolovat. 

# UAC – User account Control

