Příručka kybernetické bezpečnosti pro praktické použití

Obsah

Úvod

Tento dokument volně navazuje na teoretickou část školení a více se zaměřuje na oblasti, které je vhodné podrobněji vysvětlit a účastníkům školení je názorně demonstrovat. V první části je čtenář stručně obeznámen s problematikou práce s hesly a s důsledky jejich případného úniku. Následně je popsán postup, jak vytvářet dobrá hesla a jak lze jejich kvalitu ověřit. V závěru kapitoly je popsána práce s nástroji KeepassX a Bitwarden, dvěma populárními správci hesel.

Druhá kapitola se hlouběji věnuje problematice šifrování dat. Čtenáři jsou demonstrovány možnosti, jak zašifrovat dokument v desktopové verzi MS Office, jak ochránit několik souborů současně s využitím zaheslovaného ZIP archivu a také jak vytvářet celé šifrované svazky nástrojem VeraCrypt.

Třetí kapitola popisuje důležitost a výhody elektronického podpisu pro e-mailovou komunikaci a také postup konfigurace e-mailového klienta a následné podepisování a šifrování e-mailových zpráv.

Pravidelné aktualizace, antivirový software a firewallová ochrana by měly být nedílnou součástí každého zabezpečeného zařízení. Jak se s tím vypořádat na platformě Windows? O tom pojednává čtvrtá kapitola.

V páté kapitole je popsán význam VPN služby a postup konfigurace zařízení, aby mohlo komunikovat přes VPN bránu.

V závěrečné kapitole se dozvíte, že soubory, které vytváříme, o nás často uchovávají zbytečně mnoho informací. Čtenář je seznámen s jednoduchým způsobem, jak tyto informace odstranit.

Práce s hesly

Hesla jsou často jedinou překážkou, která zabraňuje ostatním lidem v přístupu k vašim datům, osobním informacím a financím. Pokud se neoprávněná osoba dostane jakýmkoliv způsobem k heslu, přebírá (alespoň z pohledu systému) identitu právoplatného uživatele.

Jak může heslo uniknout

- **Chyba na webovém serveru**. Útočník získá databázi uživatelských jmen a hesel. Pokud užíváte všude totožné heslo, jsou tím de-facto prolomeny všechny vaše účty. Pro prvotní získání databáze je nezbytné mít dostatečně technické znalosti, databáze uživatelských údajů však bývají běžně přeprodávány, zveřejňovány a sdíleny. Dopady takového úniku můžeme minimalizovat tím, že pro každou službu budeme používat jiné heslo.
- **Útoky hrubou silou, slovníkové útoky**. Útočník zkouší za pomocí speciálního algoritmu heslo uhádnout. Útok může probíhat pomocí slovníku - seznamu známých uniklých hesel, nebo vyzkoušením všech možných kombinací písmen a čísel. Jako obrana proti tomuto útoku je vhodné volit nepredikovatelná a dlouhá hesla. Odolnost hesel vůči útoku hrubou silou můžete vidět v tabulce.
- **Phishingový útok, sociální inženýrství**. Útočník vás zmanipuluje, abyste mu heslo sami řekli.
- **Pomocí šmírovacího malwaru**. Útočník je schopen na zařízení nainstalovat nástroje, které mu umožní zaznamenávat uživatelem stisknuté klávesy.

	8 znaků	12 znaků	15 znaků	Příklad
malá/velká písmena	35 minut	8 let	2 miliony let	pepicekk
písmena	2 dny	377 tisíc let	53 miliard let	pEpiceKk
písmena + číslice	1 rok	3 miliony let	742 miliard let	pE8ic0Kk1
písmena + číslice + speciální znaky	46 let	459 milionů let	381 trilionů let	pE8*c0Kk!

Tab. 1: Demonstrace exponenciálního navýšení strojového času nutného k uhodnutí hesla pomocí útoku hrubou silou

Kvalita hesel

Bez ohledu na způsob úniku hesla je zjevné, že útočník má k dispozici heslo, které je schopen přiřadit k určité osobě. Může tedy zkoušet, zda ona osoba nepoužila stejné heslo i k dalším službám, které využívá (např. e-mail, sociální sítě). Praxe ukazuje, že toto chování je mezi uživateli velmi časté. Uživatel by měl správně používat pro každou službu heslo jiné.

Volba hesla

Heslo lze prolomit zkoušením všech možných kombinací znaků (a, b, c, …, aa, ab, ...). Z tohoto důvodu jsou nevhodná jak hesla s příliš malou množinou znaků (6549821, vihaiuvt), tak hesla příliš krátká (@H0j). Útočník může také využít faktu, že lidé rádi používají existující slova či fráze (heslo, slunicko, LordOfTheRings), notoricky známá hesla (password, abc123, toor) nebo hesla s očividným vzorcem (12345, qwertz, asdfjklů). V neposlední řadě může útočník využít informací, které k dané osobě má - jméno, datum narození, jméno partnera, jméno psa, přezdívka, oblíbený film. Tyto informace lze jednoduše získat rychlým prohlédnutím sociálních sítí nebo pomocí sociálního inženýrství.

Dobrá hesla tedy musí být zároveň dostatečně dlouhá a dostatečně neuhodnutelná. V zásadě lze postupovat dvěma způsoby:

- dlouhá nesmyslná fráze (PlejtvakSiKoupilPrilisMaleBotyOjojoj),
- náhodná hesla, např. vygenerovaná speciálním nástrojem (b#6ArsQ8/XUh9U5e).

V heslech je typicky možné používat mezeru (útočníci s tím málokdy počítají), v některých případech však s tím může mít služba problém.

Nicneříkající frázi si zapamatujete velmi snadno, nicméně služby často definují pravidla pro tvorbu hesel (délka min. 10 znaků, alespoň jedno číslo apod.) Náhodná hesla je naopak obtížné si zapamatovat. Je tedy vhodné postupovat tak, že všechna hesla máme uložena ve

Správci hesel (klíčence), kde jsou bezpečně zašifrována, hlavní heslo ke klíčence a případně další často používaná hesla pak mají podobu fráze bez dalšího jazykového významu, a proto si je snadno pamatujeme i bez klíčenky.

Příklady

- admin - jedno z nejpoužívanějších hesel na světě
- defenestrace - existující slovo
- koupiljsemprosynovcezimnistadion
- Mnohe, co kdysi bylo, je ztraceno. - známý citát z Pána Prstenů
- qaywsxedcrfvtgbzhnujmikolp - písmena shora dolů
- zoh7rud3raiv#hChohVu
- lucinka1993 - dohledatelné osobní údaje
- WeWillRockYou! - text notoricky známé písně
- BanikPyco!!!

Ověření bezpečnosti hesla

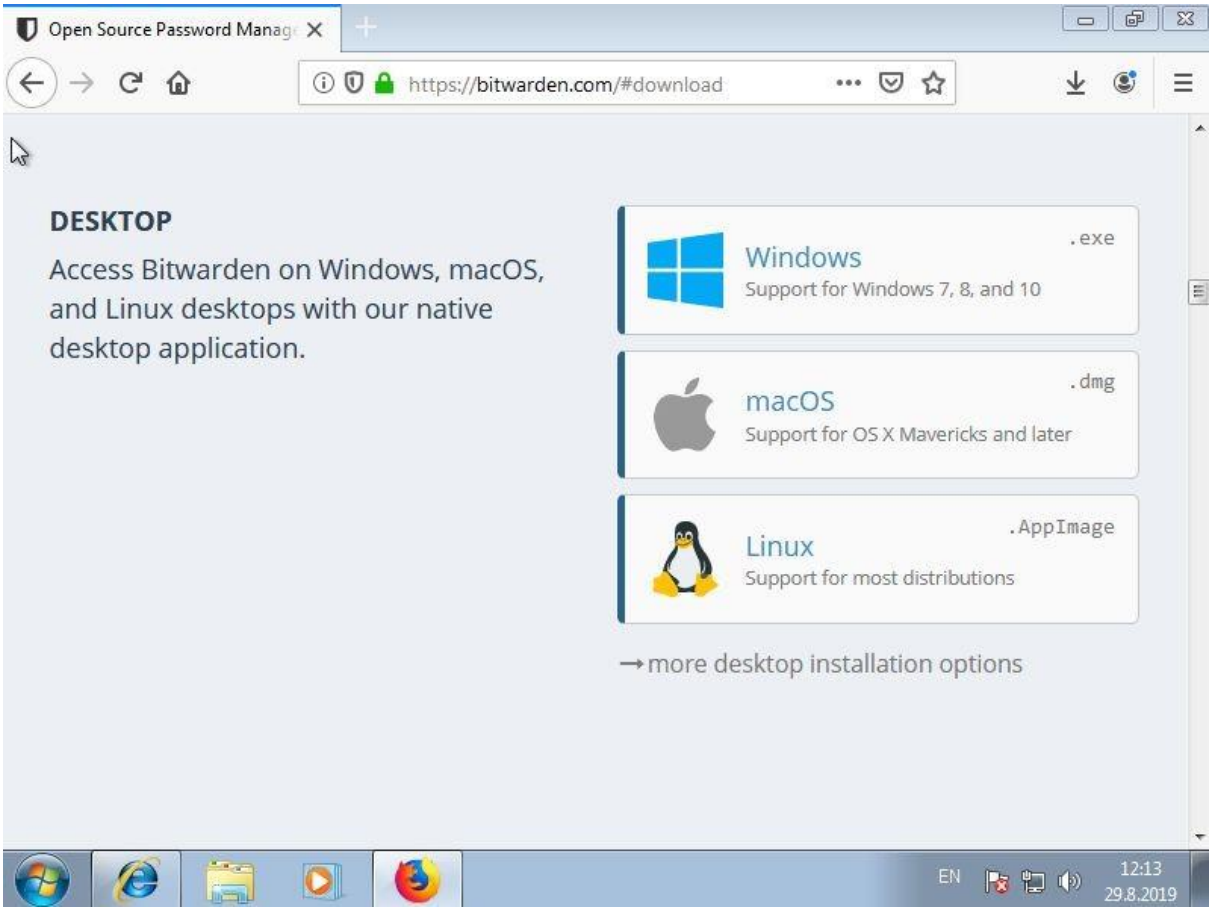
Sílu vlastního hesla je možné ověřit na stránkách https://howsecureismypassword.net/ nebo https://password.kaspersky.com/. Je vhodné *neověřovat* přesné heslo, ale heslo podobné. Stránka https://haveibeenpwned.com/ nabízí ověření, zda někdy nebyl prolomen účet s danou e-mailovou adresou.

Druhy klíčenek

Uživatel si může vybrat z několika populárních klíčenek. Existují placené varianty s omezeným používáním zdarma (1Password, LastPass, Dashlane, Bitwarden), k dispozici jsou rovněž i absolutně bezplatné produkty (Keepass2, KeepassX).
Dalším rozhodovacím kritériem je umístění dat. Hesla je možné mít umístěna v cloudu u poskytovatele služby (Bitwarden), výhodou je zejména dostupnost klíčenky z libovolných zařízení. Klíčenka též může mít podobu lokálního zašifrovaného souboru (Keepass), pro přístup z více zařízení pak musíte využít některé z cloudových úložišť (mj. OneDrive, Dropbox, Owncloud).
Zde se pokusíme objasnit způsob práce s klíčenkami KeepassX a Bitwarden.

Instalace a vytvoření klíčenky

Bitwarden je možno používat přímo z prohlížeče nebo ze specializovaných desktop aplikací. Volba je na uživateli, mobilní aplikace např. umožňuje odemknout klíčenku otiskem prstu místo zadání hlavního hesla, což je velmi komfortní. Zde ukážeme postup instalace klienta pro operační systém Windows.
Na stránkách https://bitwarden.com si v sekci *Download* zvolíte variantu pro váš operační systém. V případě problémů s instalací Windows klienta zvolte v nabídce "*more desktop installation options*" variantu *Portable App*.



Obr. 1 - webová stránka bitwarden.com

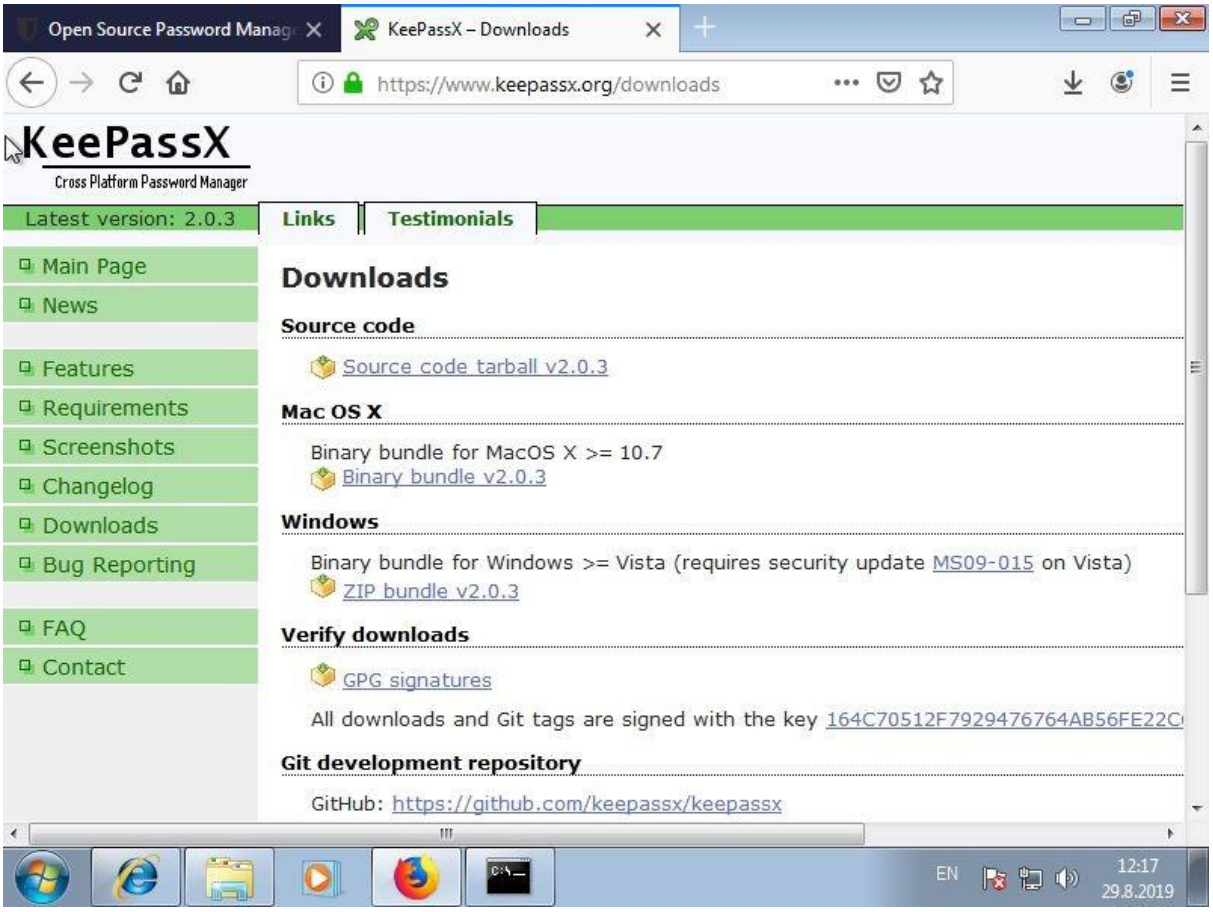
Po spuštění aplikace si založíte účet kliknutím na tlačítko *Vytvořit účet*. Po vyplnění přihlašovacích údajů se můžete přihlásit. Klíčenka je automaticky vytvořena.

Pozn. Klíčenku můžete zabezpečit dvoufázovým ověřením - při prvním přihlášení z nového zařízení bude rovněž požadován kód, který vám přijde do emailu nebo do autentizační aplikace typu Google Authenticator - ani únik hlavního hesla tak nemusí znamenat prolomení všech vašich účtů.

Obr. 2 - Bitwarden - vytvoření účtu

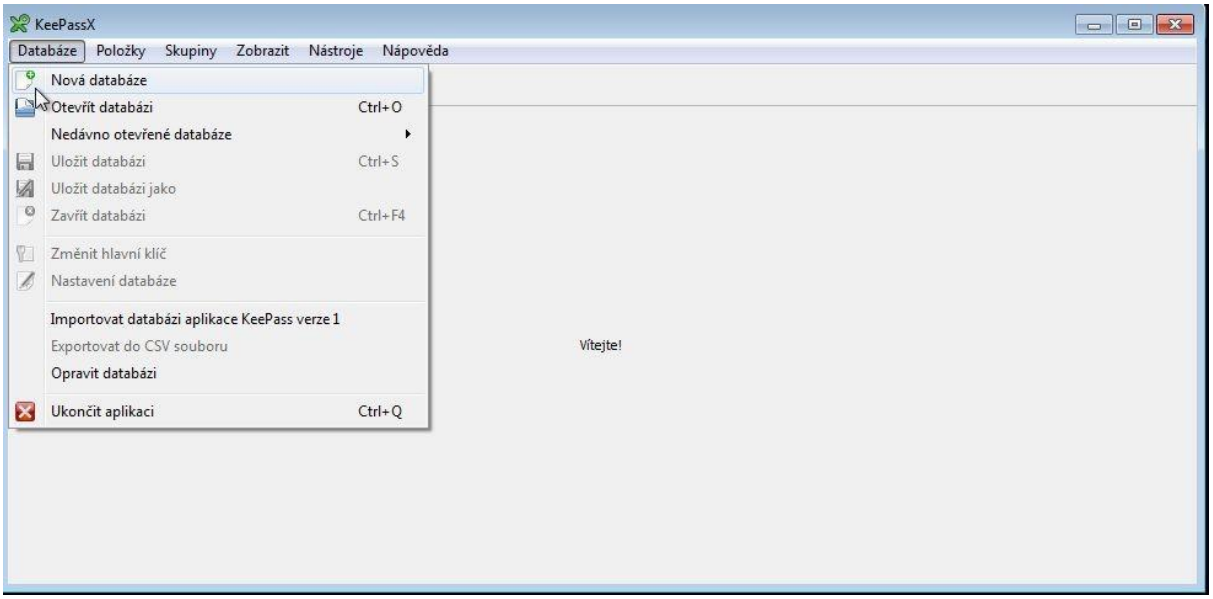
Aplikaci KeepassX si můžete stáhnout ze stránky https://www.keepassx.org ze sekce *Downloads*. Zvolte variantu pro váš operační systém.

Pro mobilní zařízení existuje více variant. Aplikace Keepass2Android umožňuje přímé připojení na nejznámější cloudové služby a také přihlašování pouhým otiskem prstu.



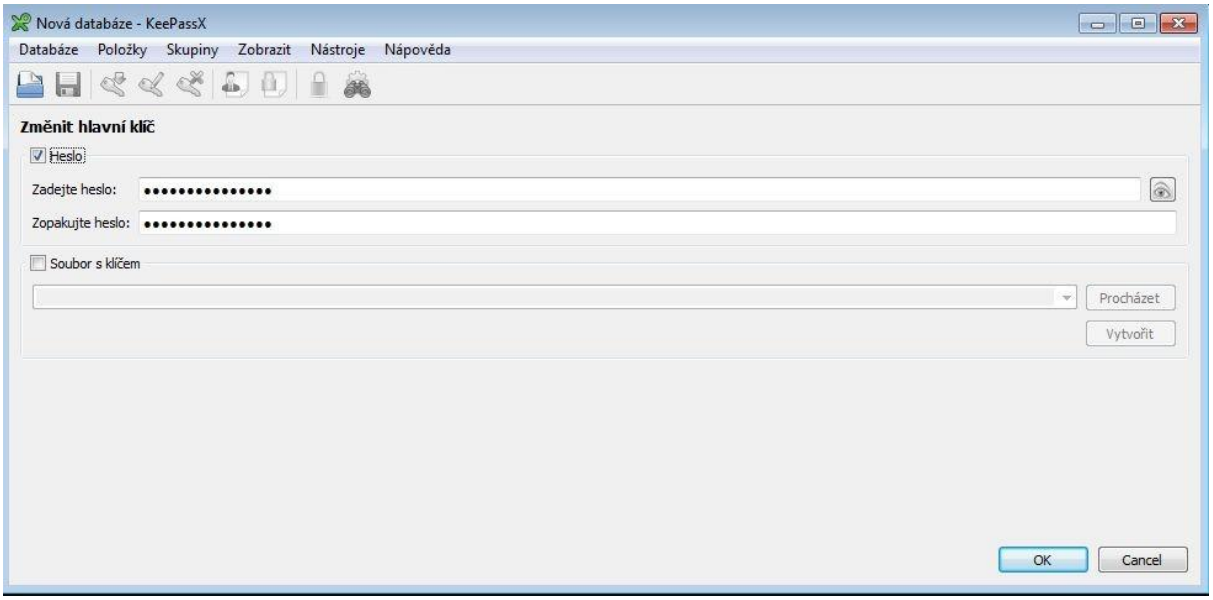
Obr. 4 - webová stránka www.keepassx.org

Po spuštění aplikace zvolte v nabídce *Databáze* možnost *Nová databáze*.



Obr. 4 - KeePassX - tvorba databáze

Následně si zvolte své hlavní heslo, musí být dostatečně dlouhé a je nutné si jej zapamatovat.

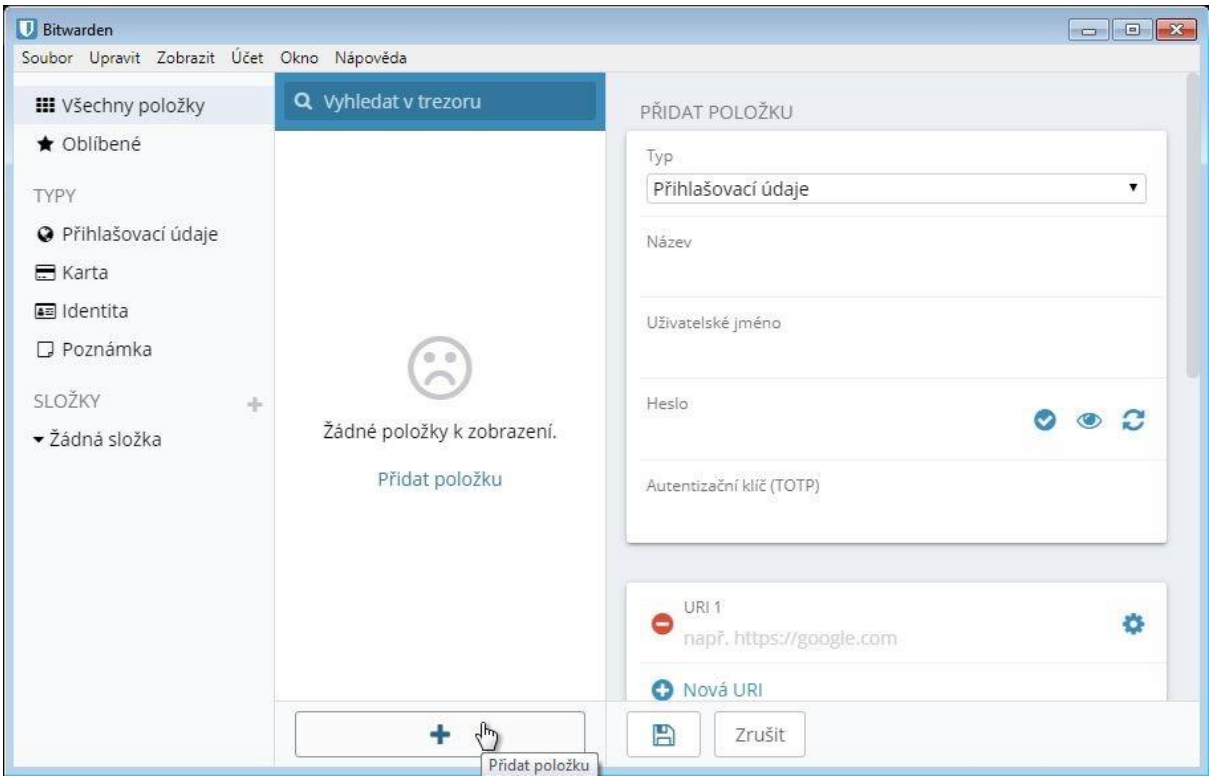


Obr. 5 - KeePassX - volba hlavního klíče

Přidání údajů do klíčenky

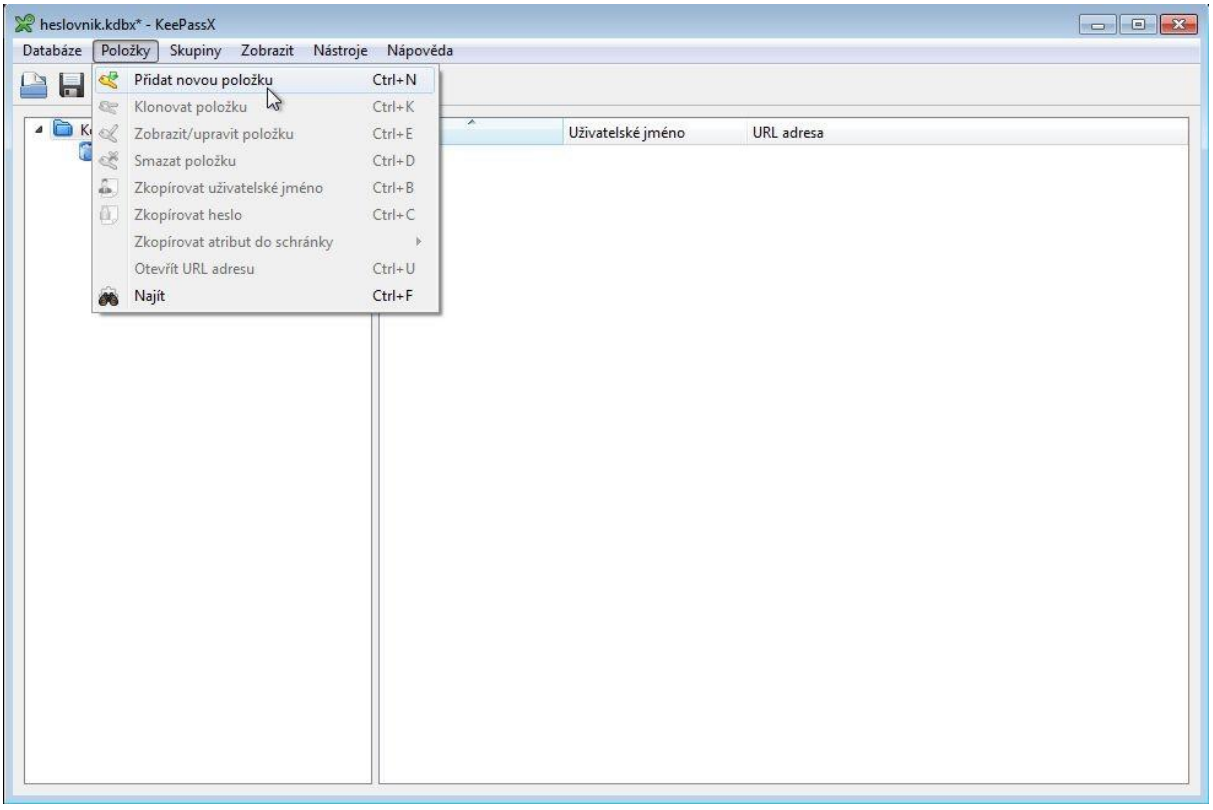
V Bitwarden aplikaci přidáte nový záznam tlačítkem +. Vpravo následně vyplníte záznam - zejména název služby, uživatelské jméno a heslo. Klíčenka vám umožňuje rovněž heslo automaticky vygenerovat - to je výhodné pro služby, které nepoužíváte moc často, např. e-shopy. Klíčenka je také schopna zkontrolovat, zda se vaše heslo nenachází v některé z uniklých databází.

V levém sloupci si můžete vytvořit složky pro různé kategorie hesel (např. pracovní, sociální sítě, bankovnictví, ...) a mít hesla přehledně uspořádána. Mezi údaji je též možné vyhledávat - zadáním části názvu služby nebo přihlašovacího jména do vyhledávacího pole nahoře. Záznam můžete upravit kliknutím pravým tlačítkem a volbou *Upravit*.



Obr. 6 - Bitwarden - přidání nové položky

Přidání nové položky do Keepass klíčenky je možné provést pomocí volby *Položky → Přidat novou položku*.



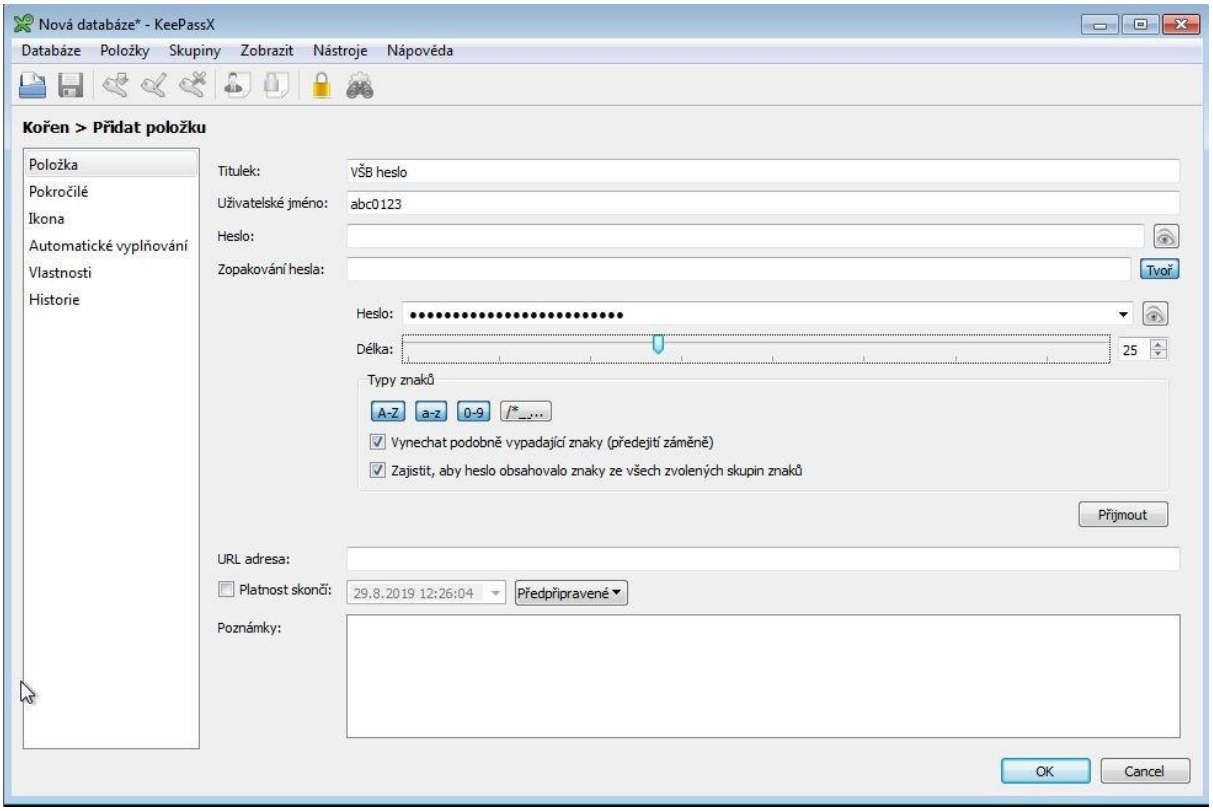
Obr. 7 - KeePassX - přidání nové položky

Následně vyplníte informace o novém záznamu - zejména titulek, uživatelské jméno a heslo. Heslo si rovněž můžete nechat automaticky vygenerovat (tlačítko *Tvoř*).

V levém sloupci si můžete vytvořit složky pro různé kategorie hesel (např. pracovní, sociální sítě, bankovnictví, ...) a mít hesla přehledně uspořádána. Mezi údaji je též možné vyhledávat - kliknutím na ikonu hledání na horní liště a následným zadáním části názvu služby nebo přihlašovacího jména do vyhledávacího pole.

Existující záznam můžete upravit pravým tlačítkem a volbou možnosti *Zobrazit/upravit položku*

.

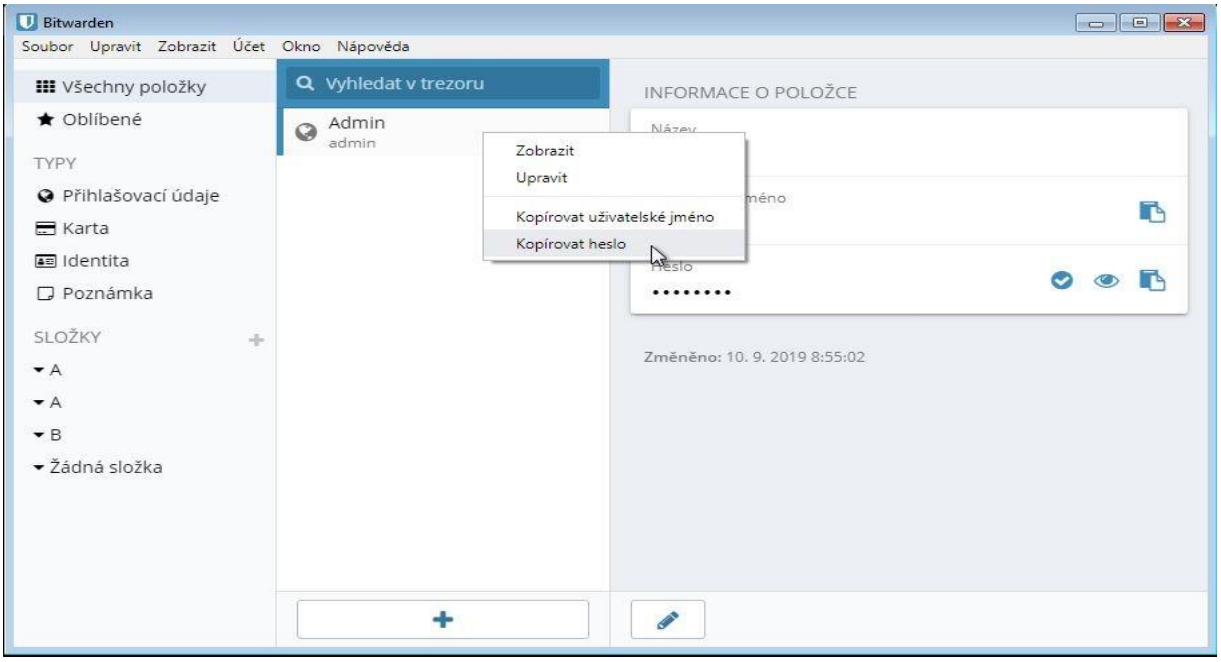


Obr. 8 - KeePassX - zadávání nových přihlašovacích údajů

Použití přihlašovacích údajů

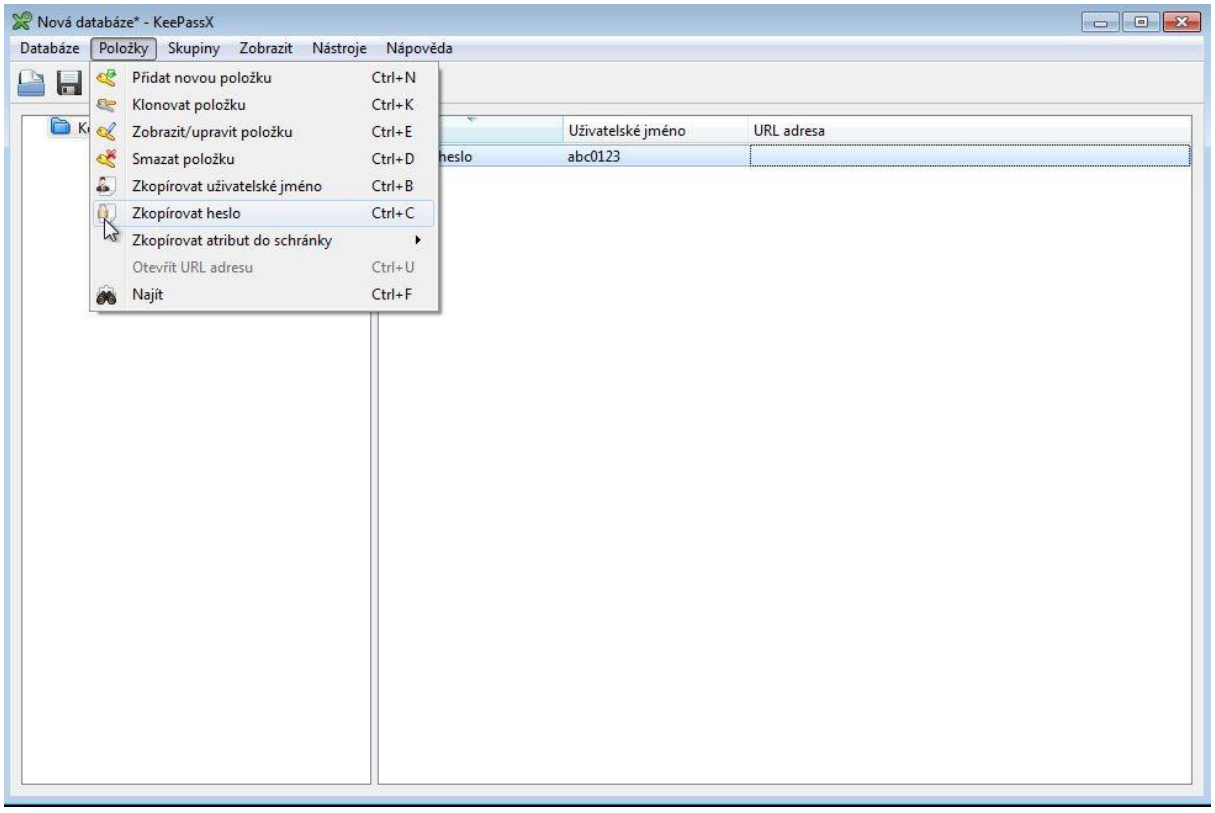
V Bitwarden klíčence kliknete na požadovaný záznam pravým tlačítkem a vyberete možnost *Kopírovat heslo*. To následně vložíte tam, kam potřebujete, a to pomocí pravého tlačítka a volby Vložit/Paste, nebo pohodlněji pomocí klávesové zkratky Ctrl+V.

Pozn. V nastavení je možné definovat čas, po kterém se zkopírované heslo ze schránky vymaže - tím je možné zabránit pozdějšímu nechtěnému vložení hesla tam, kam nepatří.



Obr. 9 - Bitwarden - manipulace s položkou

V aplikaci KeepassX vyberete záznam a následně v nabídce *Položky* zvolíte *Zkopírovat heslo*. Alternativně můžete použít klávesovou zkratku Ctrl+C, což je mnohem pohodlnější. Heslo následně vložíte tam, kam potřebujete, a to pomocí pravého tlačítka a volby *Vložit/Paste*, nebo pohodlněji pomocí klávesové zkratky Ctrl+V. Po určitém čase bude heslo ze schránky automaticky vymazáno.



Obr. 10 - KeePassX - manipulace s položkou

Uchovávání klíčenky

Klíčenka je šifrovaný soubor, proto se k obsahu nikdo bez znalosti hlavního hesla nedostane. Hlavní heslo proto musí být co nejsilnější, zároveň však dobře zapamatovatelné. V případě, že používáte klíčenku pro většinu svých hesel, může být ztráta přístupu ke klíčence velmi nepříjemná. Klíčenku na lokálním disku (Keepass) je tedy třeba zálohovat na jiné zařízení, popř. do cloudu (OneDrive, Dropbox, OwnCloud, ...) U cloudové klíčenky (Bitwarden) se o zálohování stará poskytovatel služby, pro případ nedostupnosti služby nebo nečekaných problémů je však vhodné mít i lokální kopii, jednou za čas aktualizovanou.

Šifrování

Data, která na svém počítači máte, je možné šifrovat. To znamená, že se soubory stanou absolutně nečitelnými, dokud neproběhne jejich dešifrování zadáním hesla, využitím speciálního klíče apod. Šifrovat byste měli zejména osobní data, citlivá data (faktury apod.), data na přenosných zařízeních (mobilní telefony, notebooky, USB flash disky) a data ukládaná do cloudu. Je vhodné šifrovat rovněž data, která odesíláte někomu jinému e-mailem, přes úschovnu nebo ulož.to. Některé typy souborů lze šifrovat jednotlivě (např. soubory MS Office), jiné můžete nejprve vložit do archivu a zašifrovat až ten. V této části si ukážeme nejpoužívanější a nejjednodušší způsoby šifrování.

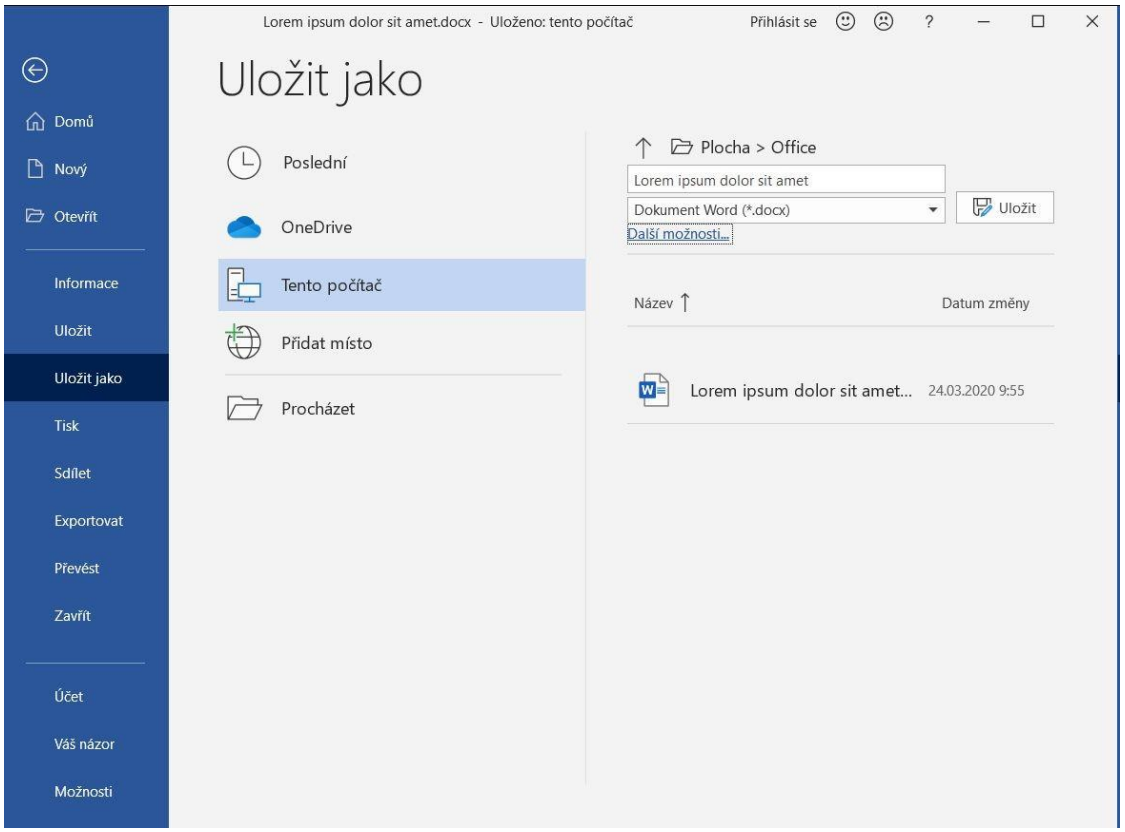
Zašifrovaná data potřebují silné heslo, které nesmíte ztratit, jinak hrozí, že se k datům již nedostanete. Uložte si proto dešifrovací heslo do vašeho správce hesel.

Některé služby pro sdílení souborů (např. ulož.to) umožňují zabezpečit soubory heslem. To vaše data může do jisté míry chránit před ostatními uživateli, ale služba samotná k datům přístup má. Soubory tedy raději šifrujte ještě před sdílením.

Dokumenty MS Office

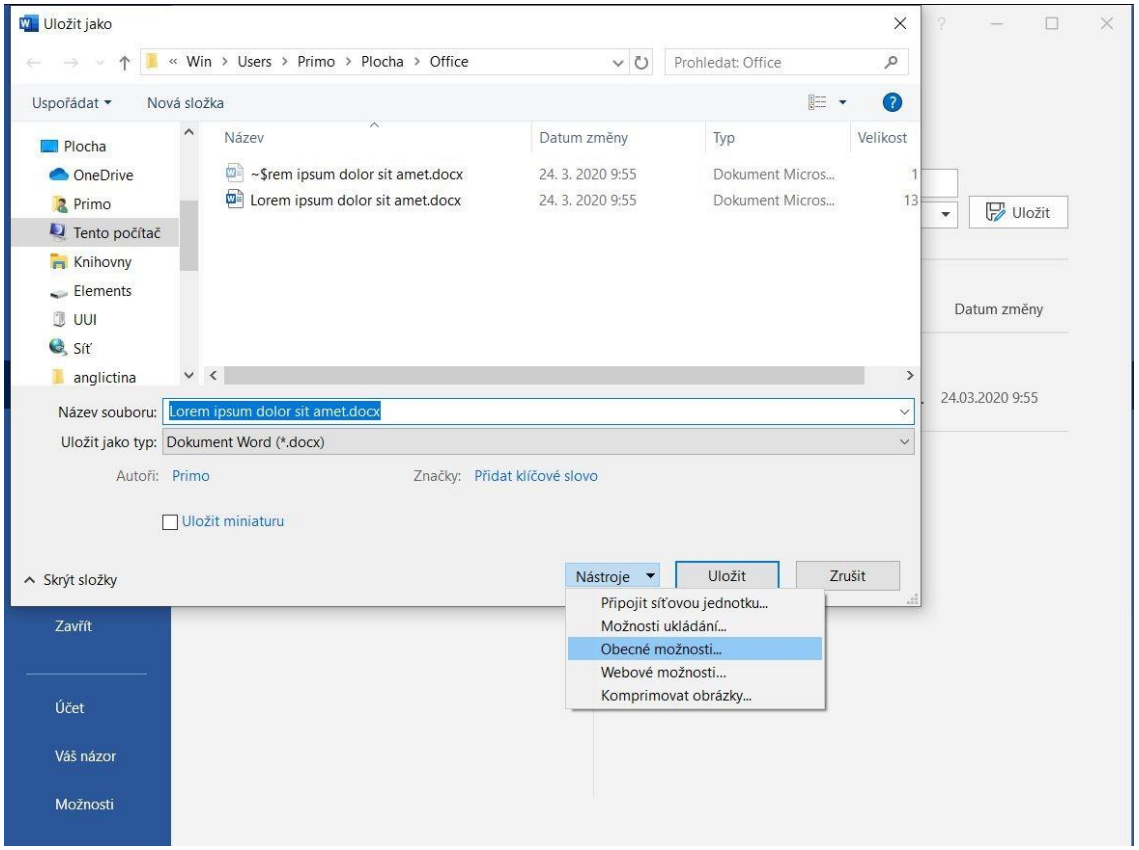
Nástroje MS Office v desktopové verzi umožňují nastavit ochranu dokumentů heslem. Ve všech typech MS Office dokumentů se ochrana nastavuje stejným způsobem, zde tedy bude popsán způsob pouze pro jeden typ souborů - dokument aplikace Word.

Ochrana heslem se nastavuje v dialogu ukládání. V hlavní nabídce je tedy nutné zvolit možnost *Soubor → Uložit jako* a následně zvolit položku *Další možnosti*.



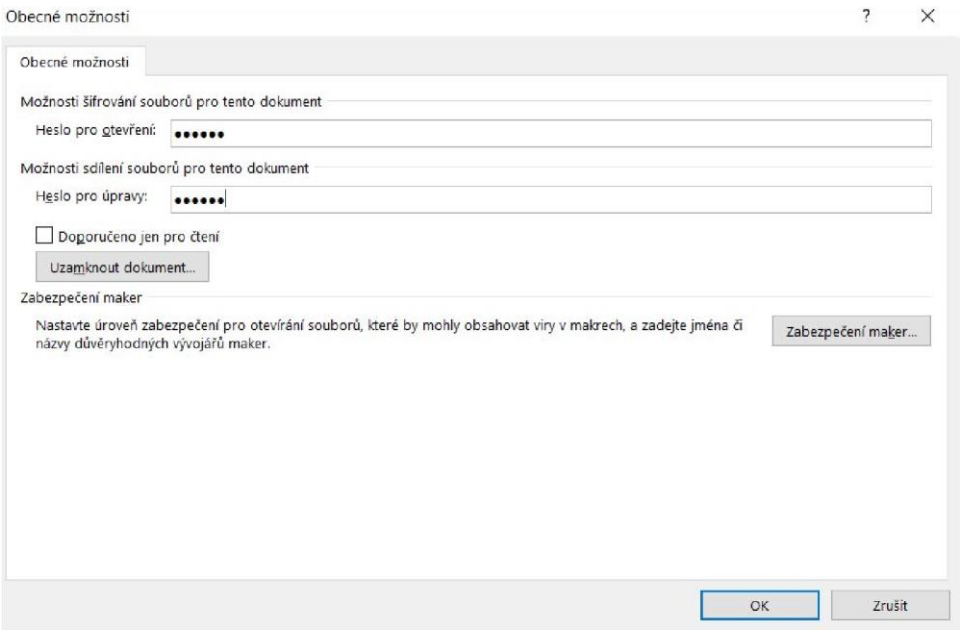
Obr. 11 - nabídka Uložit jako v MS Word 2016

V dialogu se pod tlačítkem *Nástroje* skrývá volba *Obecné možnosti*.



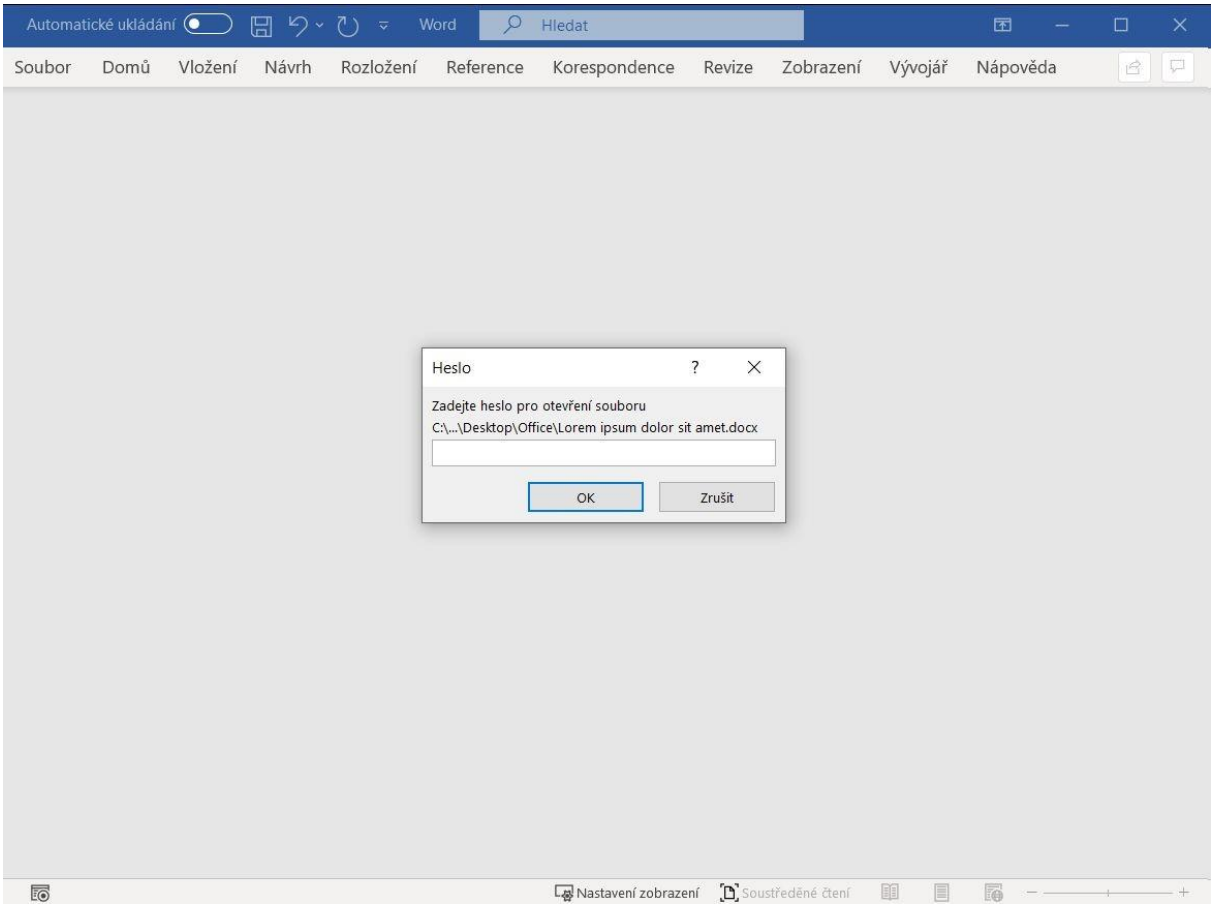
Obr. 12 - dialogové okno Uložit jako v MS Word

Do textového pole *Heslo pro otevření* se zadává heslo, které je při otevírání dokumentu vyžadováno. Rovněž můžete specifikovat *Heslo pro úpravy*. Hesla by měla být silná.



Obr. 13 - volba hesel pro ochranu dokumentů

To je vše. Při následném otevření budete vyzváni k zadání hesla.



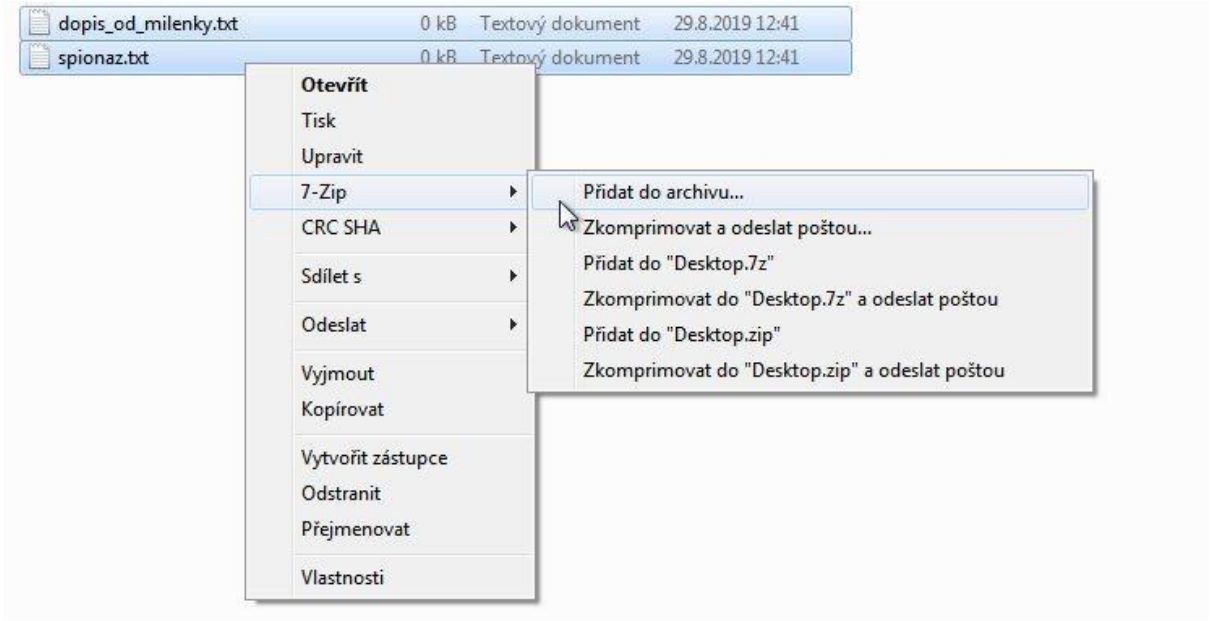
Obr. 14 - pokus o otevření zaheslovaného dokumentu

Archivy (zip)

Archivy jsou navrženy tak, aby do nich bylo možné “zabalit” více souborů. Windows umí s archivy pracovat automaticky, ale pro podporu vytváření zaheslovaných archivů je nutné doinstalovat pokročilejší aplikaci - např. 7-Zip (https://www.7-zip.org).

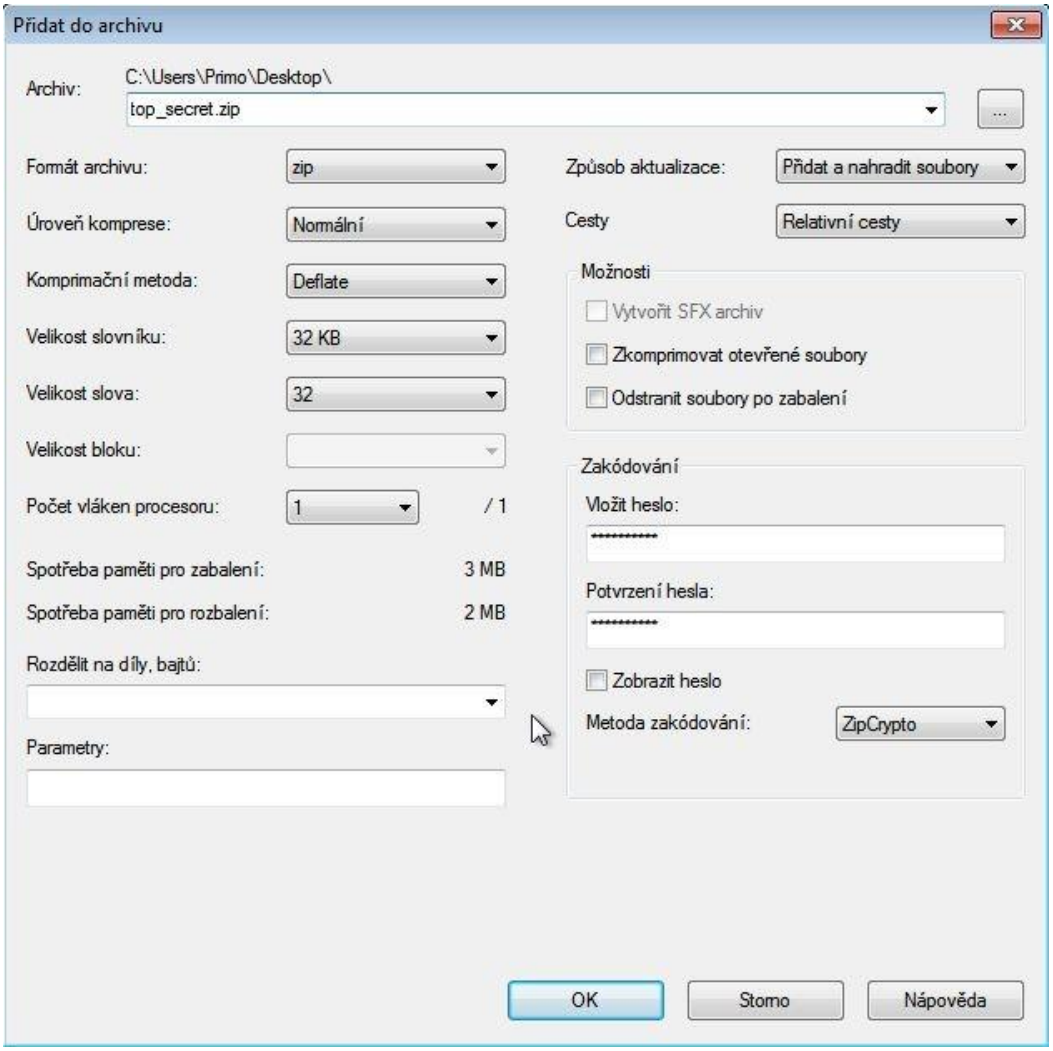
Obr. 15 - webová stránka www.7-zip.org

Po instalaci je do kontextové nabídky přidána volba *7-Zip*. Pak je možné vybrat soubory, které mají být zabaleny do archivu, vyvolat kontextovou nabídku (pravým tlačítkem myši) a zvolit možnost *7-Zip → Přidat do archivu...*



Obr. 16 - 7-Zip - tvorba archivu z kontextové nabídky

V levé části vyvolaného okna je možné zvolit *Formát archivu* - je dobré používat ZIP, který bývá univerzálně podporován. V pravé části okna lze nalézt textová pole pro zadání hesla. Heslo by mělo být dostatečně silné. Jako metodu zakódování ponechte hodnotu ZipCrypto - je nejvíce podporovaná na většině zařízení.



Obr. 17 - 7-Zip - konfigurace nového archivu

Po potvrzení dialogového okna bude archiv chráněn heslem. Bude možné jej otevřít (a tedy mimo jiné číst názvy souborů), ale při pokusu o otevření některého souboru bude nutné zadat heslo.

Tento způsob šifrování je vhodný pro přeposílání citlivých souborů kolegům. Heslo jim nezasílejte spolu s archivem, ale sdělte je jiným způsobem - nejlépe osobně, případně přes SMS.

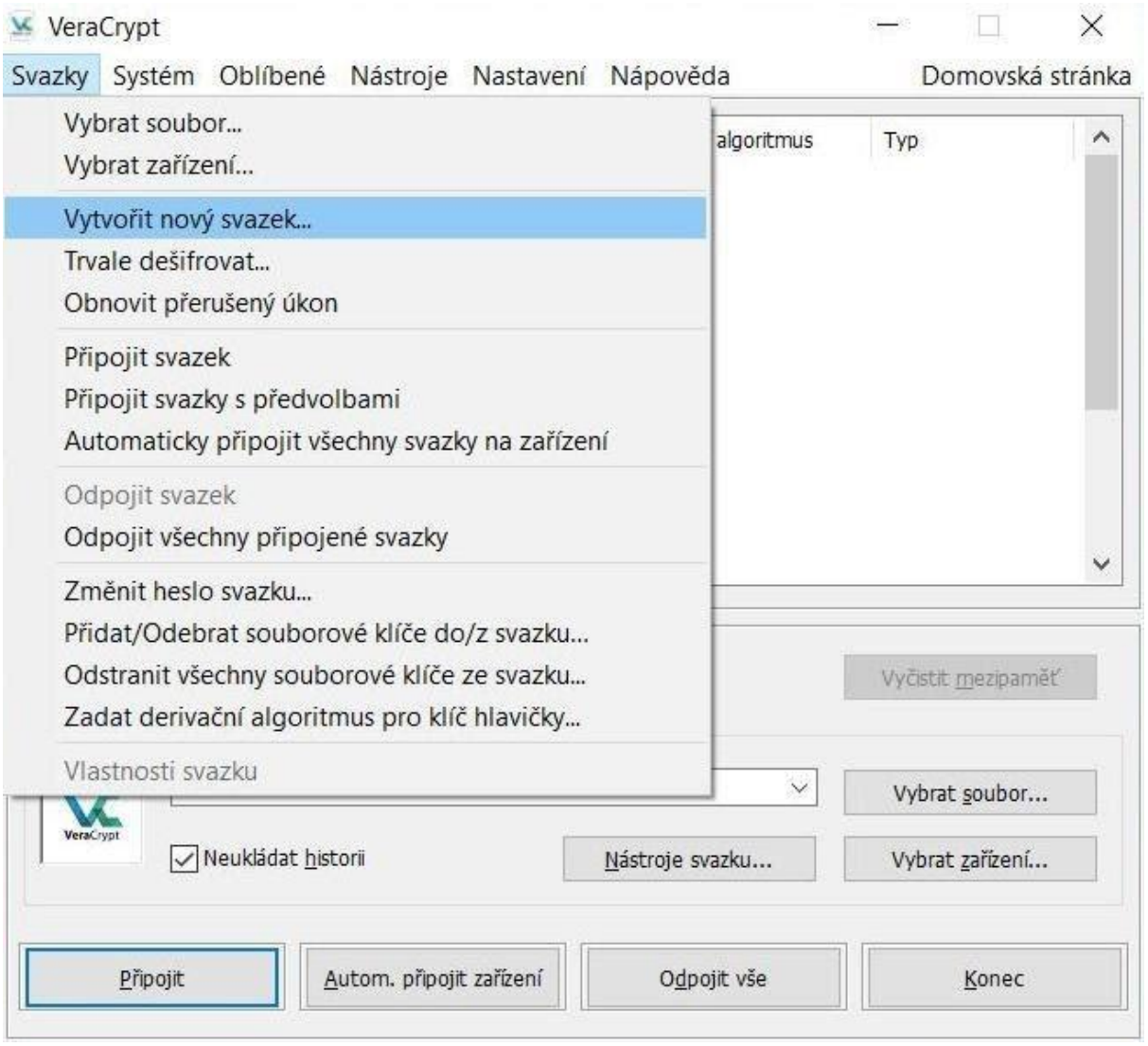
VeraCrypt

VeraCrypt je populární open-source řešení pro šifrování svazků navazující na dnes již nepodporovaný TrueCrypt.
Práce s VeraCrypt svazky je o mnoho jednodušší než práce s archivy - připojený svazek se objeví jako nový diskový oddíl, pro uživatele je tedy šifrovací mechanismus zcela transparentní. Pouze je nutné při připojování VeraCrypt svazku zadat heslo.

VeraCrypt umožňuje šifrovat celý diskový oddíl, a to i v případě, že obsahuje data. Takto je možné např. vytvořit šifrovaný flash disk nebo si na počítači vytvořit oddíl pro citlivá data.

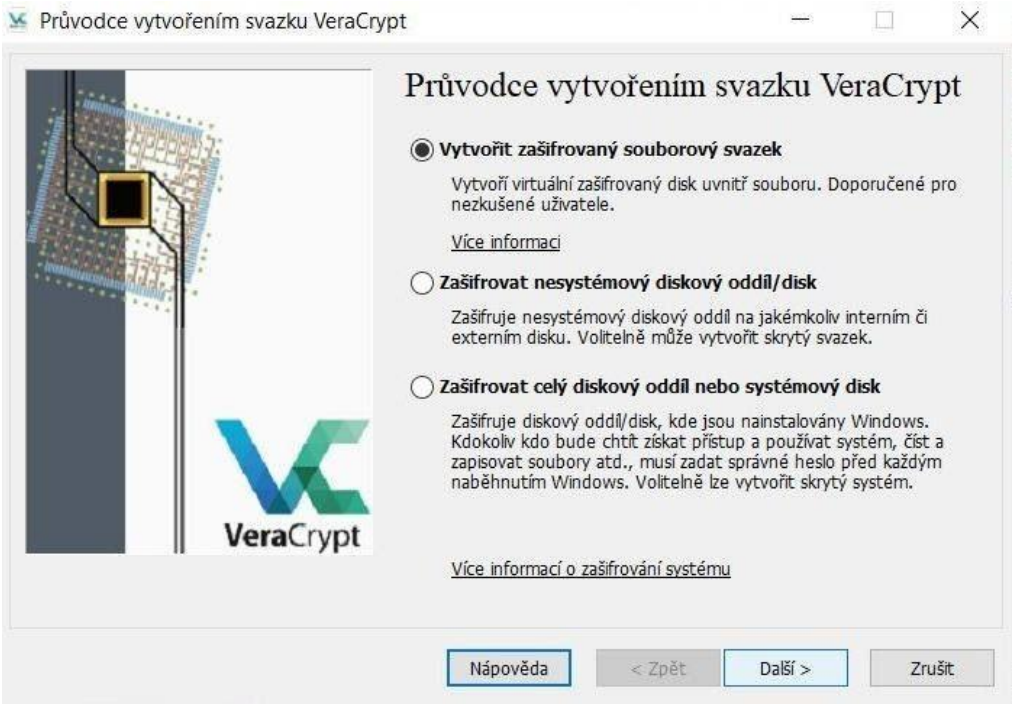
Dále je možné vytvořit *souborový svazek* - jeden velký soubor pevné velikosti, který bude mít vlastnosti archivu, do kterého se data budou ukládat.
VeraCrypt je podporován všemi běžně používanými operačními systémy. Pro otevření jakéhokoliv typu VeraCrypt svazku je však nutné mít nainstalovanou odpovídající aplikaci (https://www.veracrypt.fr/en/Downloads.html).

Po spuštění aplikace se nový svazek vytvoří volbou *Svazky → Vytvořit nový svazek*.



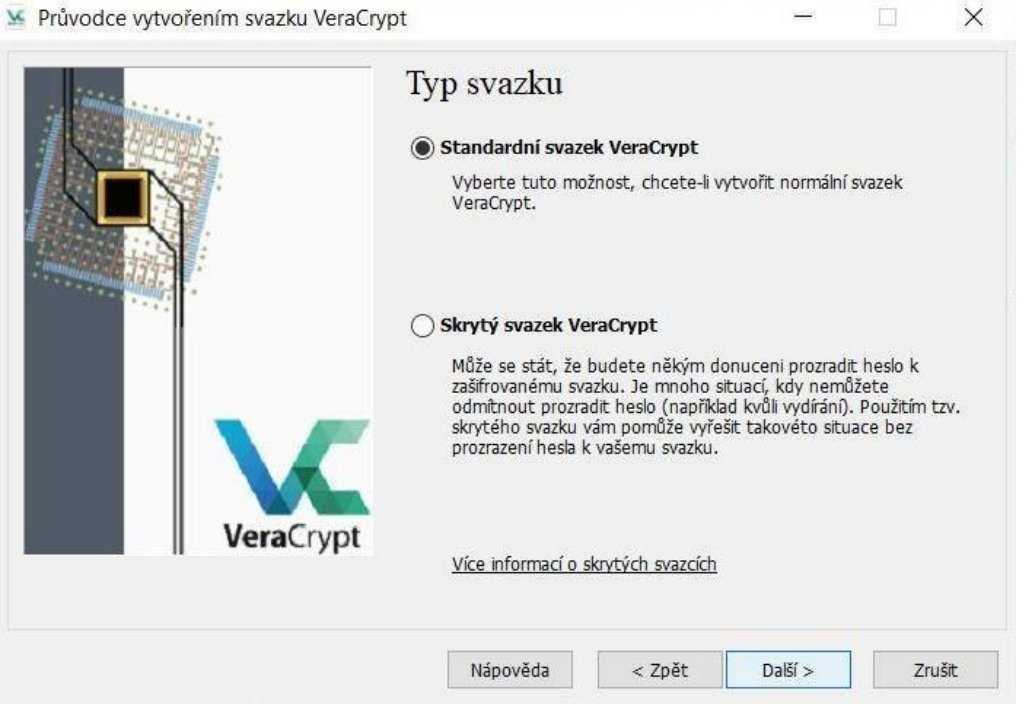
Obr. 18 - VeraCrypt - tvorba nového svazku

Poté se spustí průvodce pro vytvoření svazku. Nejdříve se vybere druh svazku (souborový svazek = soubor, diskový oddíl bez operačního systému, diskový oddíl se systémem Windows). Zde bude popsána první volba.



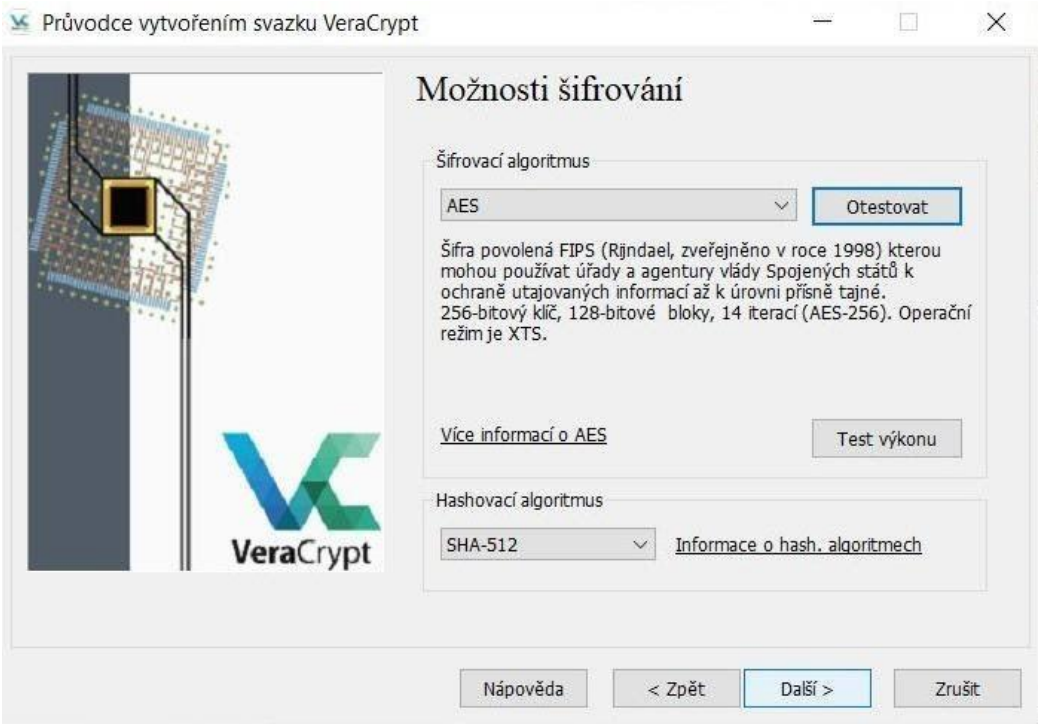
Obr. 19 - Průvodce vytvořením svazku VeraCrypt

Jako typ svazku zvolíme *Standardní svazek VeraCrypt*. Zvolíme umístění, kde bude svazek uložen.



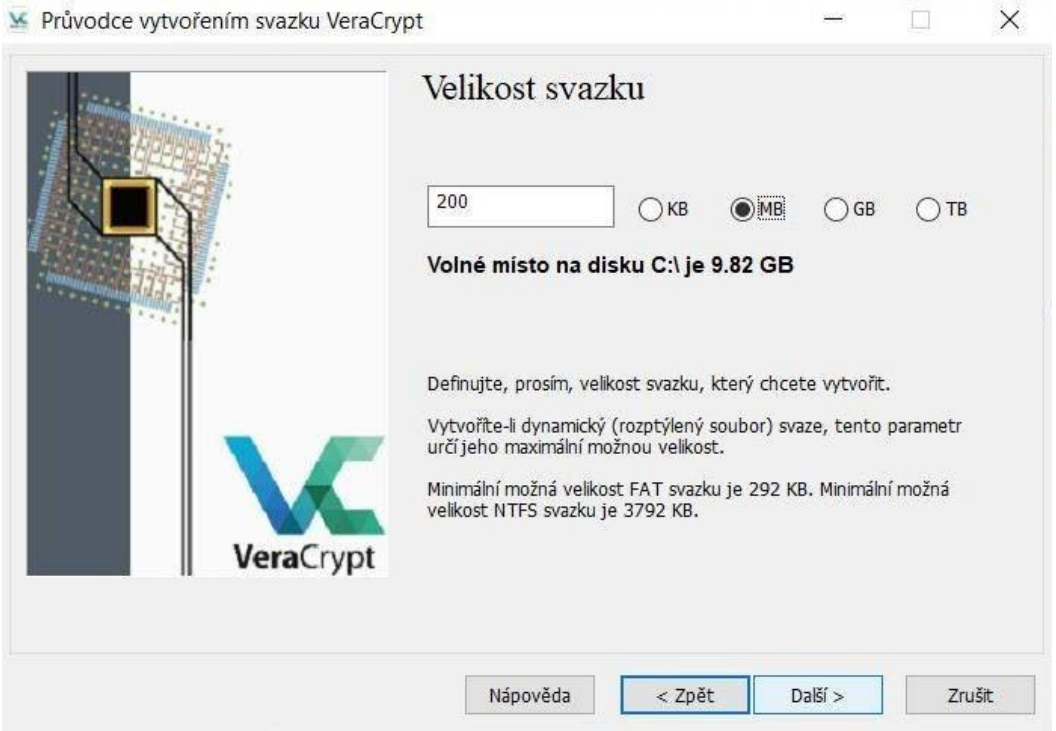
Obr. 20 - Průvodce vytvořením svazku VeraCrypt - typ svazku

Je možné specifikovat šifrovací algoritmy - můžeme ponechat původní nastavení (AES, SHA-512), které je vyhovující.



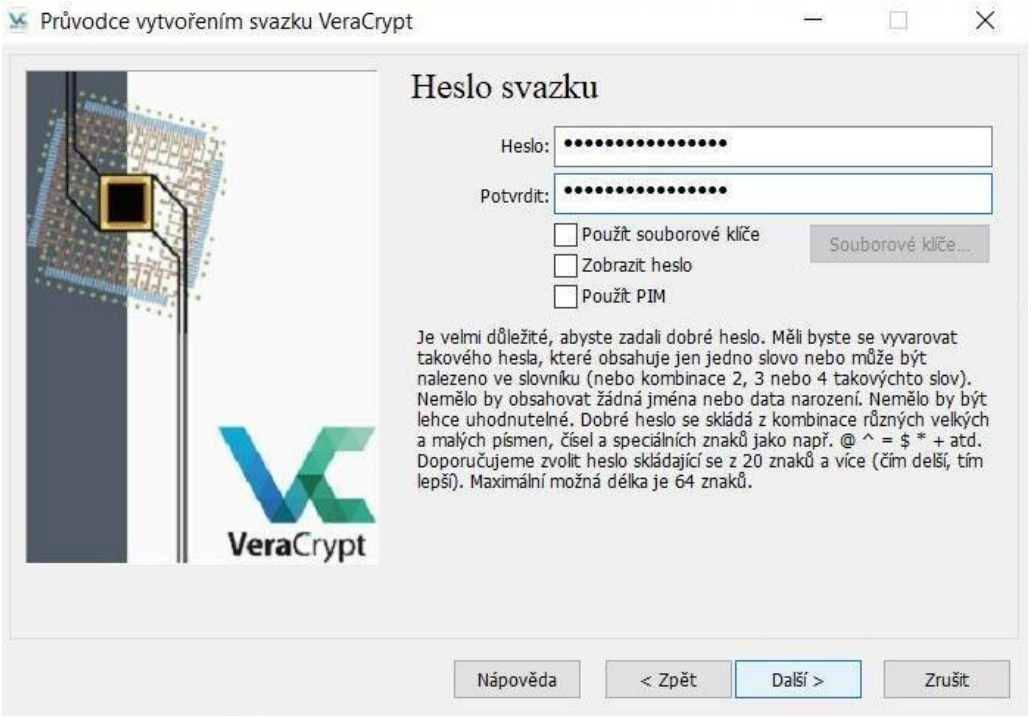
Obr. 21 - Průvodce vytvořením svazku VeraCrypt - možnosti šifrování

Dále je nutné zvolit velikost výsledného svazku. Velikost nebude možné později navýšit. Je možné vytvořit svazek dynamický, který bude zabírat pouze potřebné množství místa a s novými daty jeho velikost bude růst až do maximální definované velikosti, ale tím se bezpečnost šifrování i rychlost radikálně snižují.



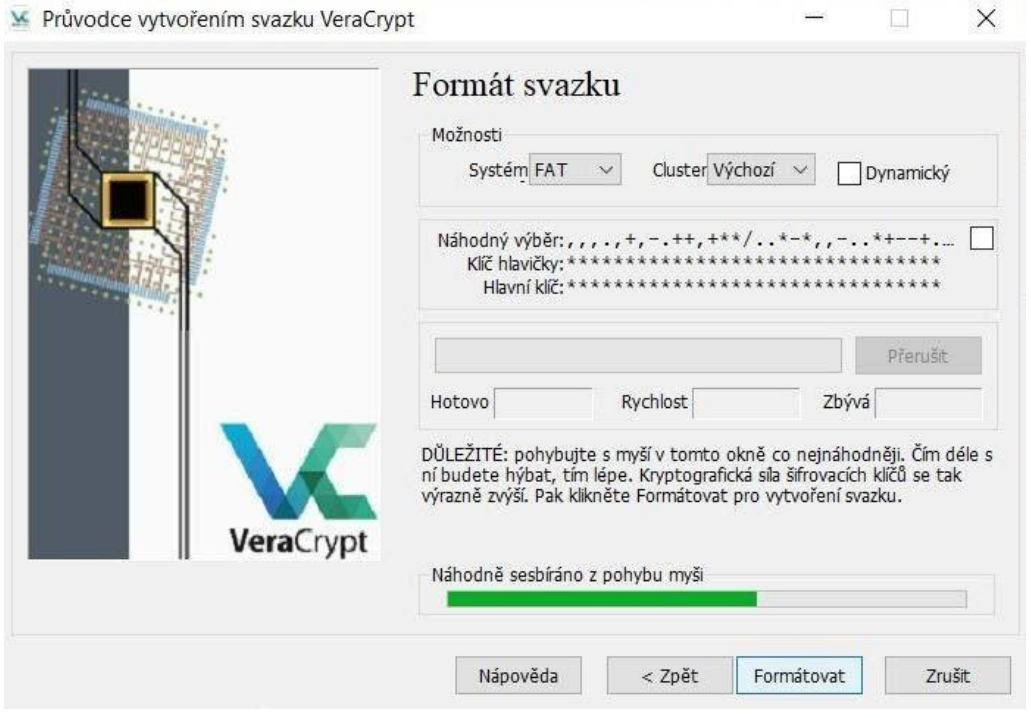
Obr. 22 - Průvodce vytvořením svazku VeraCrypt - velikost svazku

Následně je nutné zvolit si OPRAVDU SILNÉ heslo.



Obr. 23 - Průvodce vytvořením svazku VeraCrypt - heslo svazku

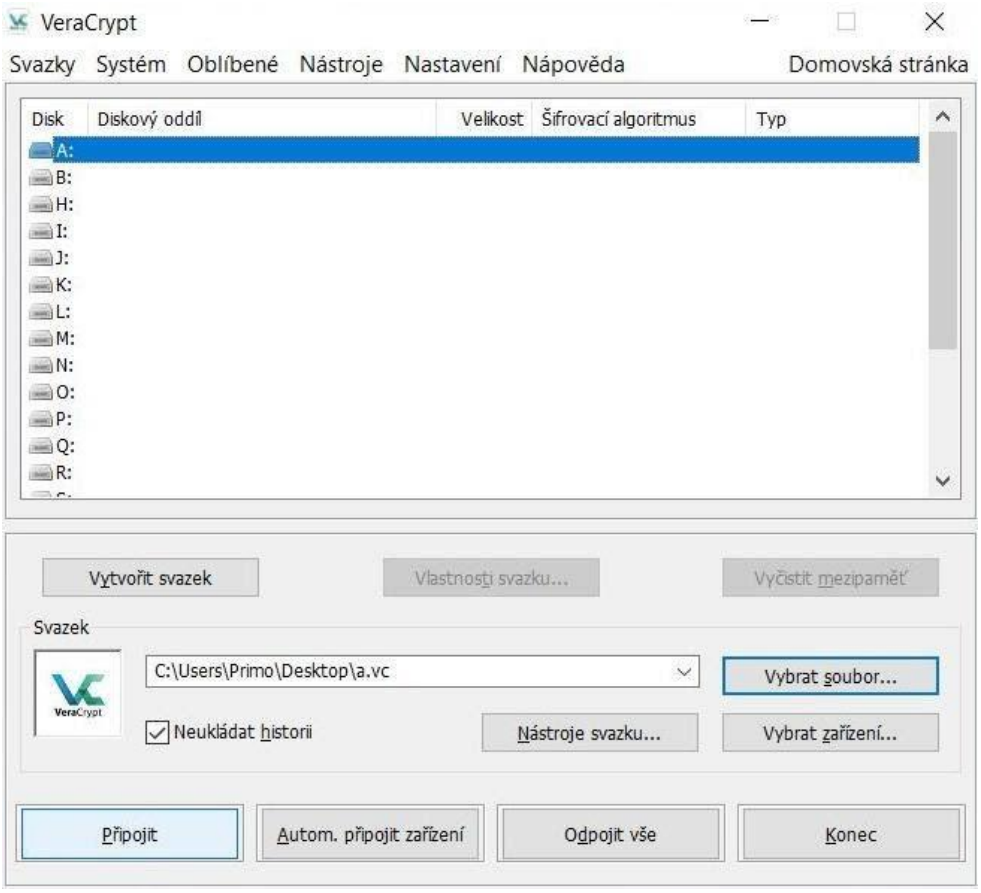
Dále musíme zvolit souborový systém - na systémech Windows je dobré zvolit FAT nebo ještě lépe NTFS. VeraCrypt následně vygeneruje hlavní klíč sbíráním pseudonáhodných dat (např. pohybů myši). Čím silnější hlavní klíč bude vygenerován, tím lépe budou data chráněna.



Obr. 24 - Průvodce vytvořením svazku VeraCrypt - formát svazku

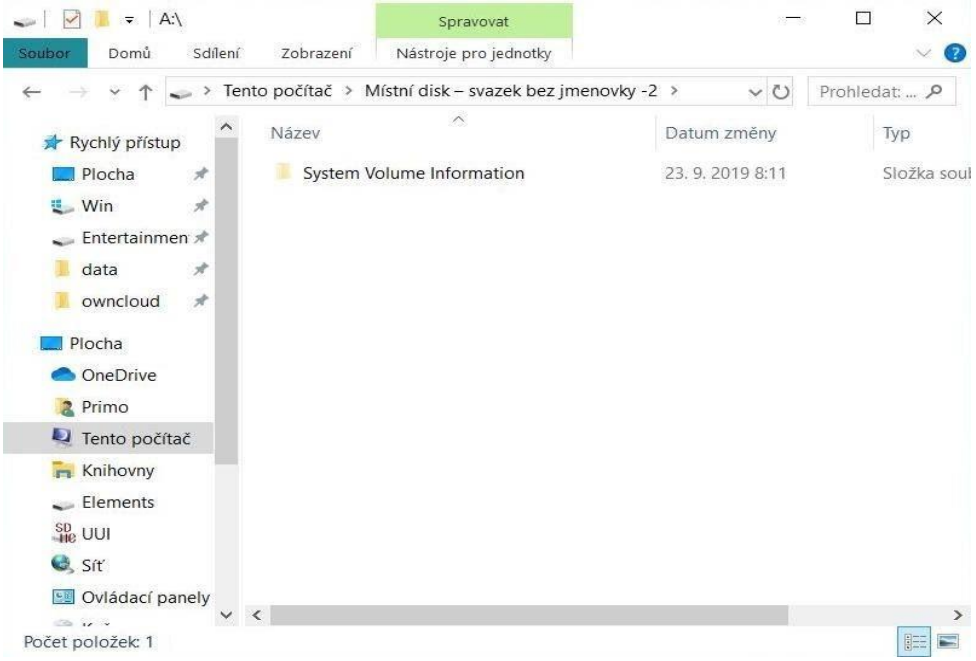
Po formátování je VeraCrypt svazek vytvořen.

Svazek se připojí v hlavním okně VeraCryptu volbou písmena disku, stisknutím tlačítka *Vybrat soubor*, vybráním vytvořeného kontejneru a stisknutím tlačítka *Připojit*. Následně budete vyzváni k zadání hesla.



Obr. 25 - VeraCrypt - připojení svazku

Po zadání správného hesla se svazek zobrazí jako nový připojený disk (podobně jako flash disk) a lze se do něj dostat například přes *Tento počítač*.



Obr. 26 - Připojený svazek v Průzkumníku Windows

Elektronický podpis

Při obdržení e-mailové zprávy máme tendenci předpokládat, že jejím odesílatelem byla osoba, která je na konci zprávy podepsaná. Tento předpoklad je velmi špatný, je totiž zřejmé, že do obsahu zprávy může kdokoli napsat cokoli. Je nutné kontrolovat adresu odesílatele zprávy (pole From), ale ani to nestačí. Fakt, že při odesílání lze jednoduše změnit adresu odesílatele je málo znám, nicméně útočníky je hojně využíván. Jediným řešením je proto využít tzv. elektronický podpis - mechanismus matematicky zajišťující, že pole From je platné. Vlastník elektronického podpisu může rovněž přijímat šifrované e-maily.

Jak zažádat o elektronický podpis

Organizacím, které jsou připojeny do EduID.cz (sdružení CESNET) je k dispozici vydávání certifikátů zdarma. Pro vytvoření certifikátu navštivte stránku https://tcs.cesnet.cz/, zvolte záložku Osobní certifikát a postupujte podle pokynů. V dalším kroku certifikát exportujte ze svého prohlížeče (postup se bude lišit).

Pozn. V květnu 2020 došlo ke změně poskytovatele certifikačních služeb a aktuálně probíhá úprava portálu pro vydávání těchto certifikátů. Očekáváme brzké spuštění provozu.

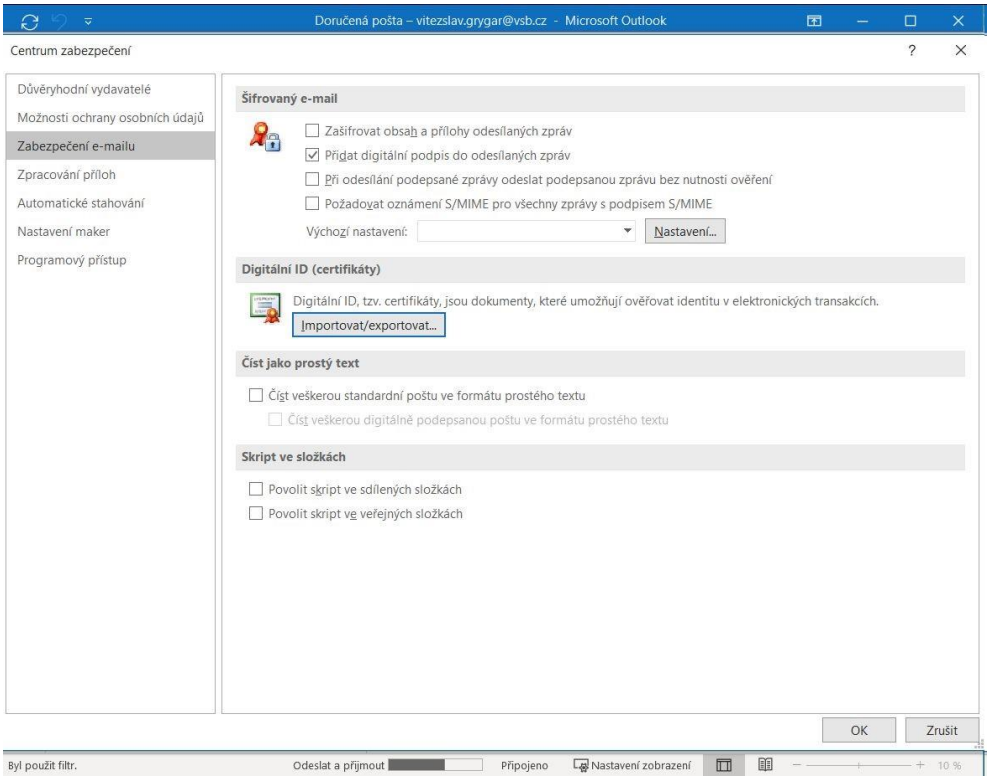
Pro komunikaci s orgány státní správy a jinými institucemi může být vyžadován kvalifikovaný elektronický podpis, jehož vydávání je zpoplatněno.

Nastavení elektronického podpisu v e-mailových klientech

Získaný certifikát musí být importován do e-mailového klienta. Zde uvádíme postup konfigurace v klientech Microsoft Outlook a Mozilla Thunderbird.

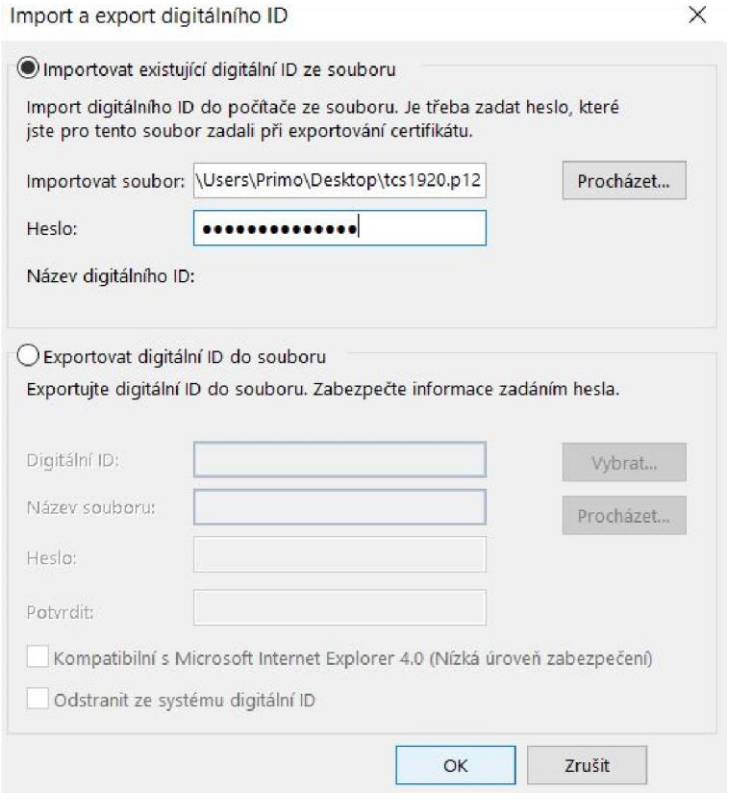
Microsoft Outlook

Importování podpisového certifikátu do Outlooku se provádí v Centru zabezpečení: *Soubor → Možnosti → Centrum zabezpečení → Nastavení centra zabezpečení → Zabezpečení e-mailu*
.



Obr. 27 - Konfigurace zabezpečení e-mailu v MS Outlook

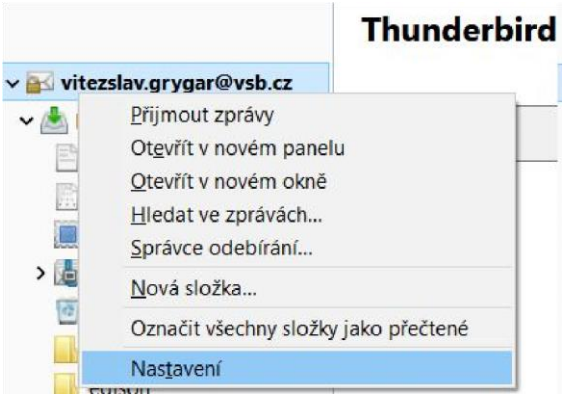
Zaškrtněte možnost "*Přidat digitální podpis do odesílaných zpráv*" a následně klikněte na tlačítko *Importovat/Exportovat*. V zobrazeném dialogu doplňte cestu k vašemu exportovanému certifikátu a zadejte heslo.



Obr. 28 - Import digitální identity v MS Outlook

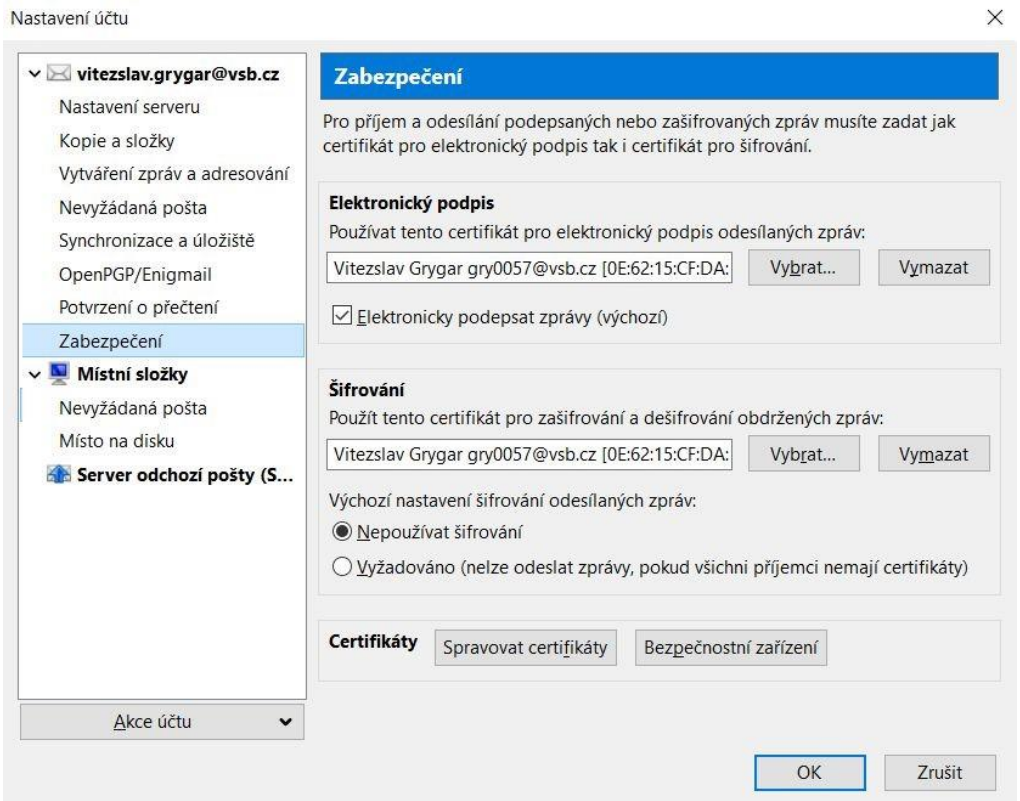
Mozilla Thunderbird

Importování podpisového certifikátu do Thunderbirdu se provádí v nastavení účtu. Do nastavení se dostanete kliknutím pravým tlačítkem myši na Váš účet a výběrem položky *Nastavení*.



Obr. 29 - Nastavení účtu v Mozilla Thunderbird

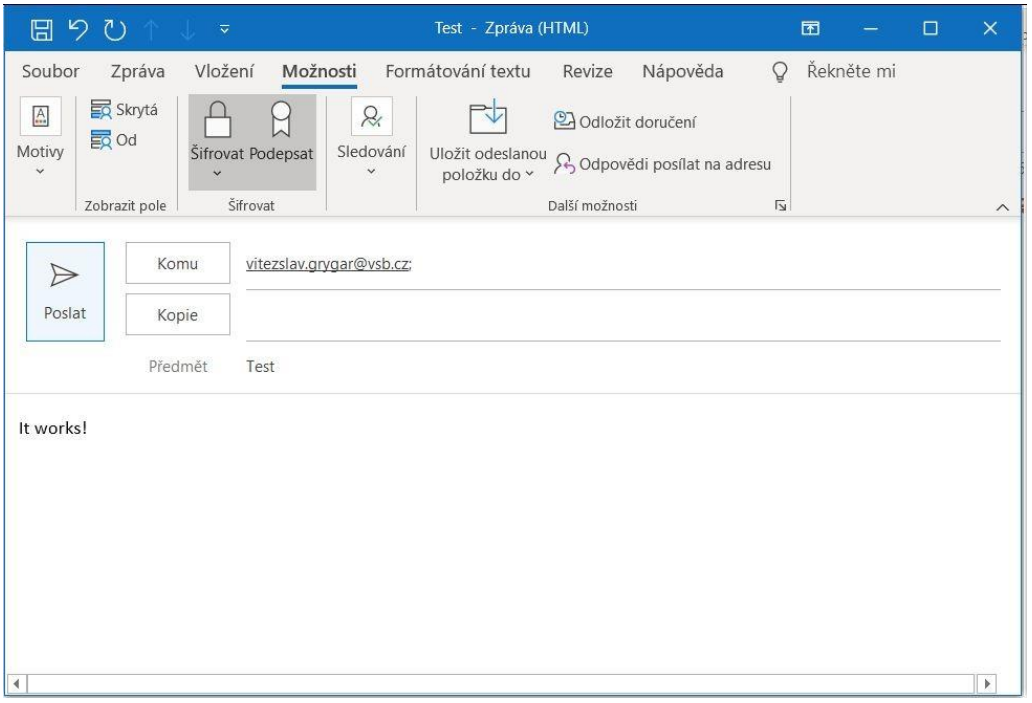
V záložce *Zabezpečení* naleznete nastavení vztahující se k podepisování a šifrování. Zde zvolíte certifikát, který má být k těmto účelům používán (import certifikátu je možné provést kliknutím na tlačítko *Spravovat certifikáty*). Následně nechte zaškrtnutou volbu *Elektronicky podepsat zprávy (výchozí)*.



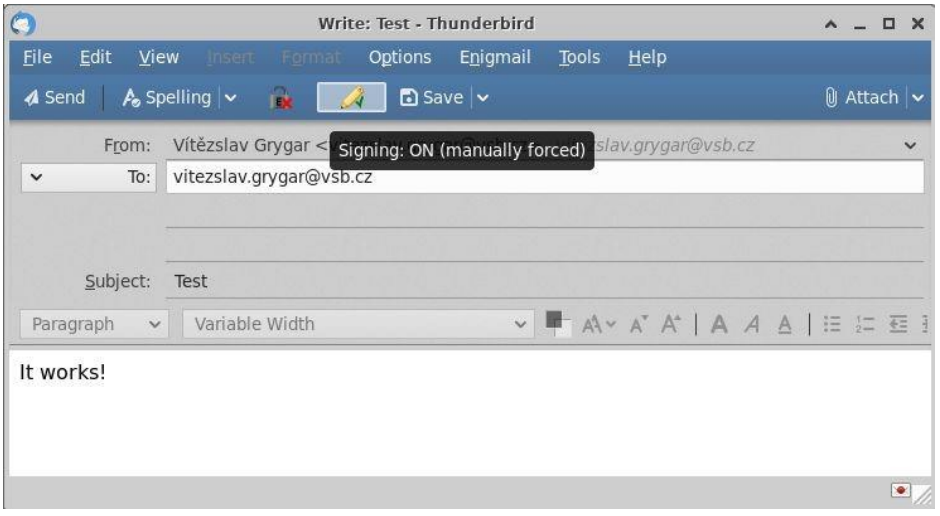
Obr. 30 - Záložka Zabezpečení v Mozilla Thunderbird

Jak podepisovat a šifrovat e-maily

Při psaní e-mailu nyní uvidíte v Thunderbirdu na horním panelu zvýrazněné tlačítko pro podepisování a vlevo od něj tlačítko pro šifrování. V Outlooku se tato tlačítka nacházejí na kartě *Možnosti*. Šifrovat zprávu můžete pouze v případě, že jste od příjemce již obdrželi alespoň jeden podepsaný e-mail - e-mailový klient Vás upozorní, pokud nebude šifrování možné.



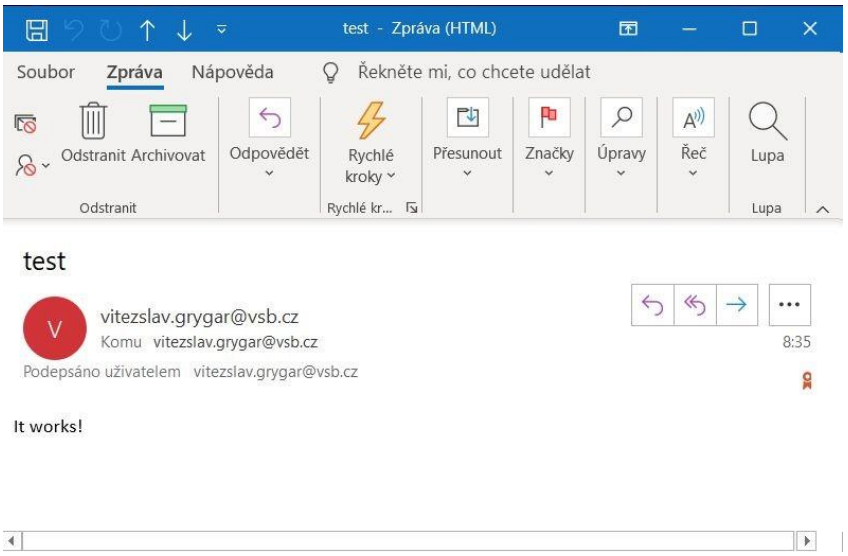
Obr. 31 - Tvorba zprávy v MS Outlook



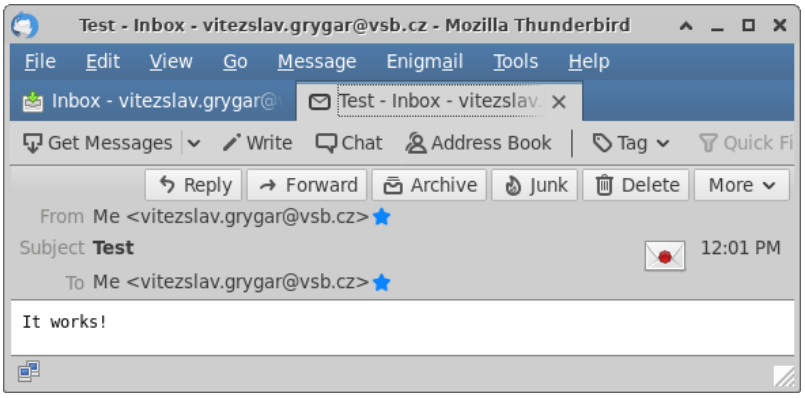
Obr. 32 - Tvorba zprávy v Mozilla Thunderbird

Jak zkontrolovat platnost elektronicky podepsané zprávy

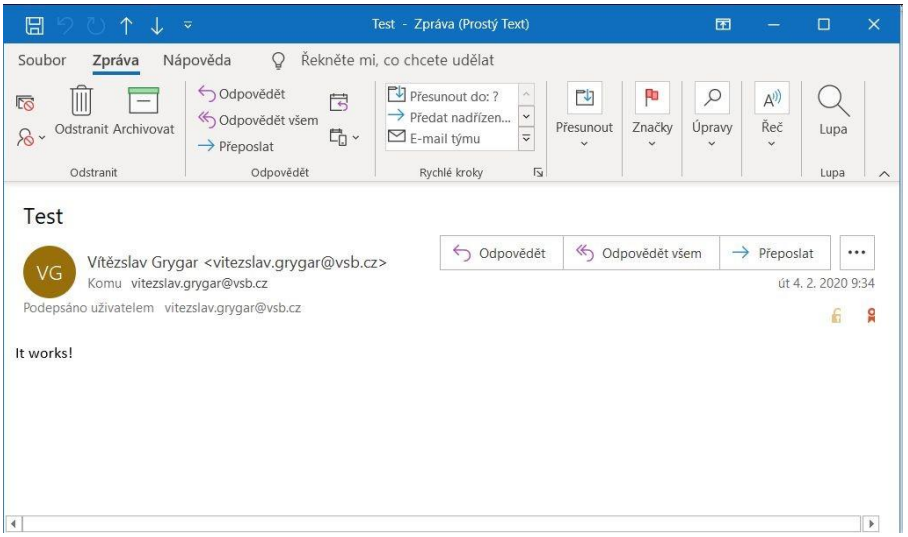
Zprávy podepsané platným podpisem jsou označeny pečetí (Outlook) nebo zapečetěnou obálkou (Thunderbird). Šifrované e-maily budou označeny ikonou zámku.



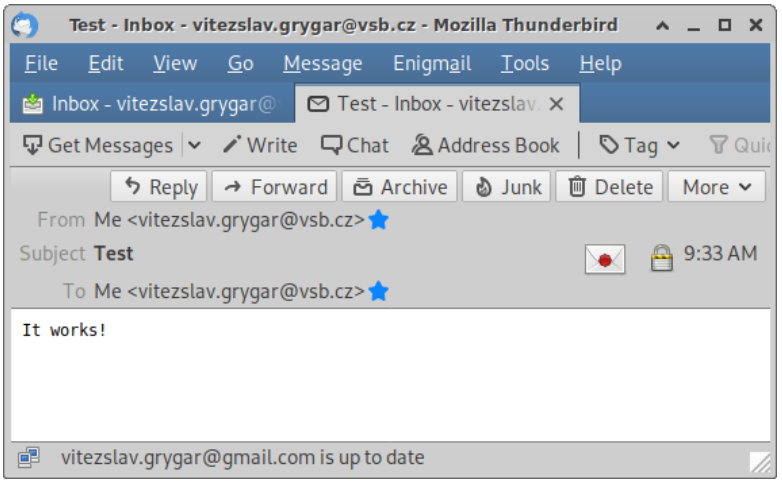
Obr. 33 - Elektronicky podepsaný e-mail označen pečetí (MS Outlook)



Obr. 34 - Elektronicky podepsaný e-mail označen zapečetěnou obálkou (Thunderbird)



Obr. 35 - Podepsaný a šifrovaný e-mail označen zámkem a pečetí (MS Outlook)



Obr. 36 - Podepsaný a šifrovaný e-mail označen zámkem a zapečetěnou obálkou (Thunderbird)

U podepsaného e-mailu máte jistotu, že zpráva opravdu přišla od odesílatele (pole From) a že zprávu po cestě nikdo neupravoval. U šifrovaného e-mailu máte jistotu, že si jej při zasílání nikdo nepřečetl.

Ochrana zařízení

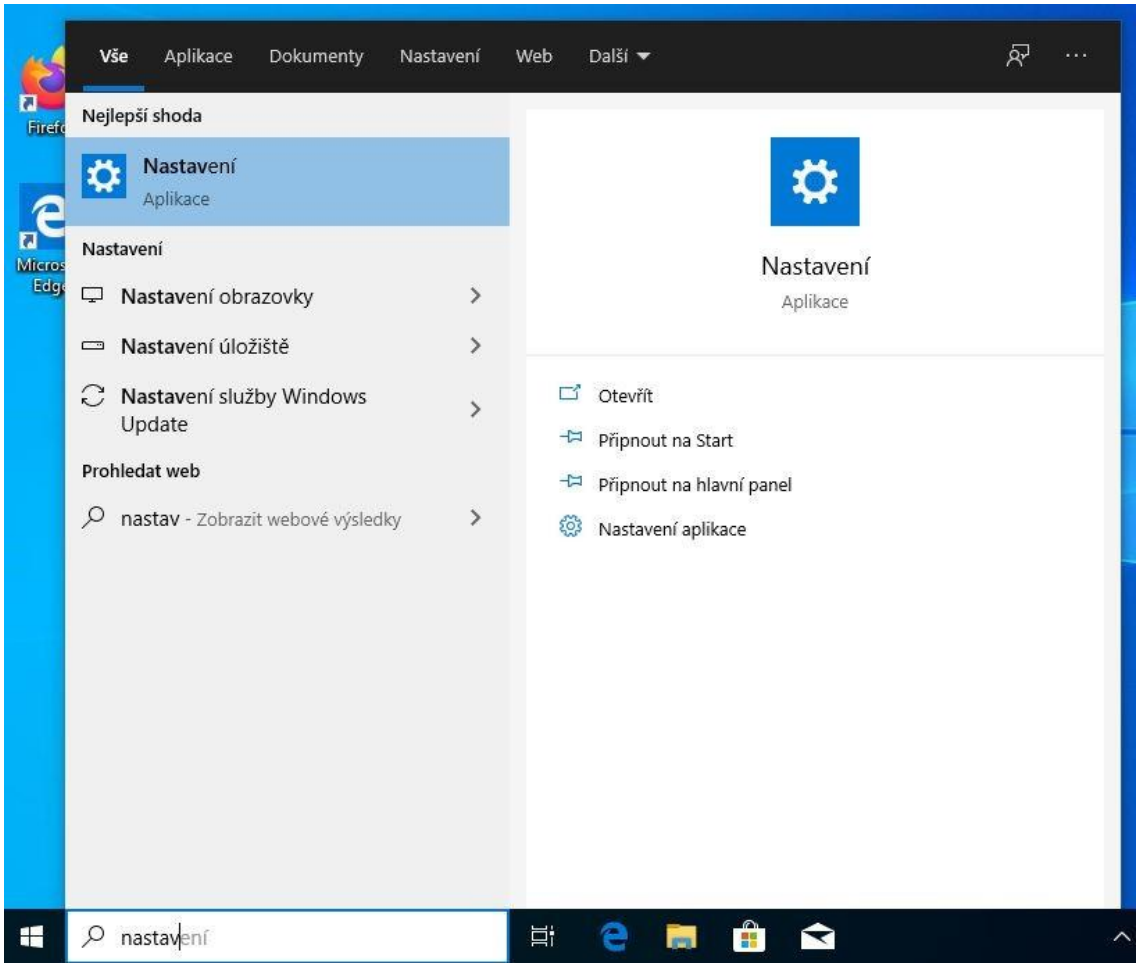
Aby bylo vaše zařízení chráněno, musí splňovat několik podmínek:

- musí mít antivirovou ochranu - pro likvidaci škodlivého kódu, který se do počítače dostane,
- musí být chráněno firewallem - pro omezení přístupu ke službám počítače z počítačové sítě,
- musí být aktualizováno - aby útočník nemohl zneužít chybu:
    - ve službě, která z důvodu funkcionality nemůže být omezena firewallem,
    - v prohlížeči, přes který se k vám může dostat škodlivý kód,
    - v samotném systému.

Žádné řešení neposkytuje stoprocentní ochranu, je proto nezbytné chránit zařízení na všech úrovních.

Aktualizace

Pokud chcete zkontrolovat aktualizace na vašem zařízení, je třeba spustit systémovou aplikaci *Nastavení*. Tu můžete vyhledat pomocí vyhledávacího pole na hlavní liště.

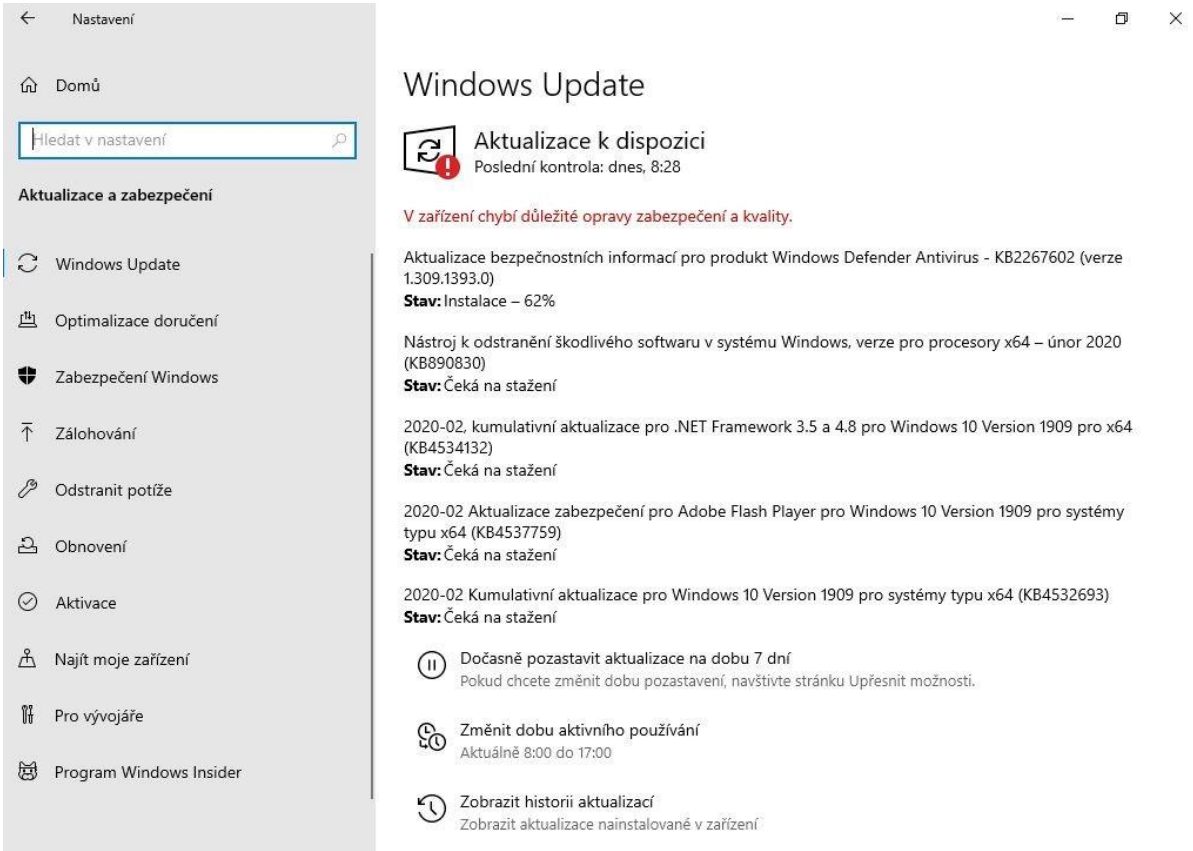


Obr. 37 - Vyhledávání aplikací ve Windows 10

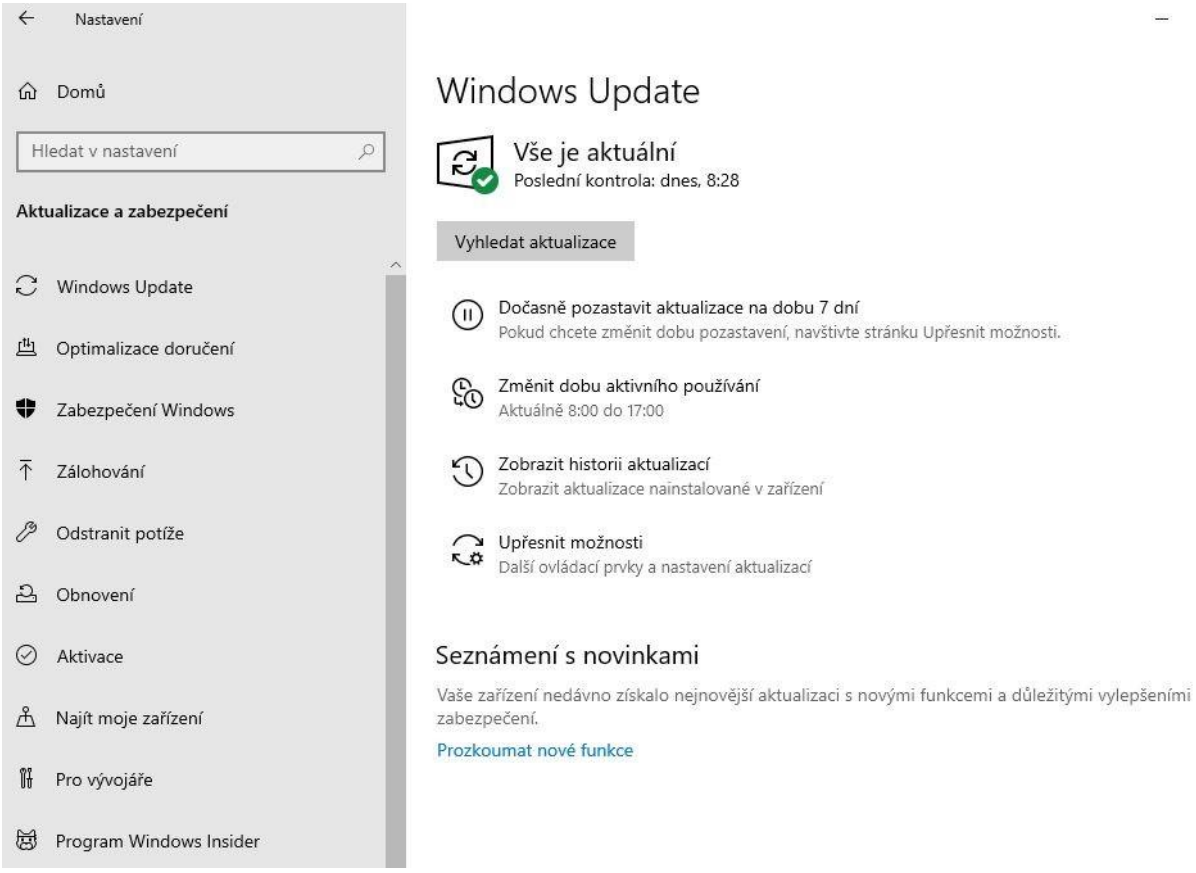
V nabídce Nastavení vyberete položku *Aktualizace a zabezpečení*.

Obr. 38 - Nastavení ve Windows 10

Informace o systémových aktualizacích se zobrazí jako první položka. Zde můžete zkontrolovat, zda je váš systém aktualizován, které aktualizace selhaly a můžete zde ručně vynutit aktualizace, které ještě nebyly nasazeny.



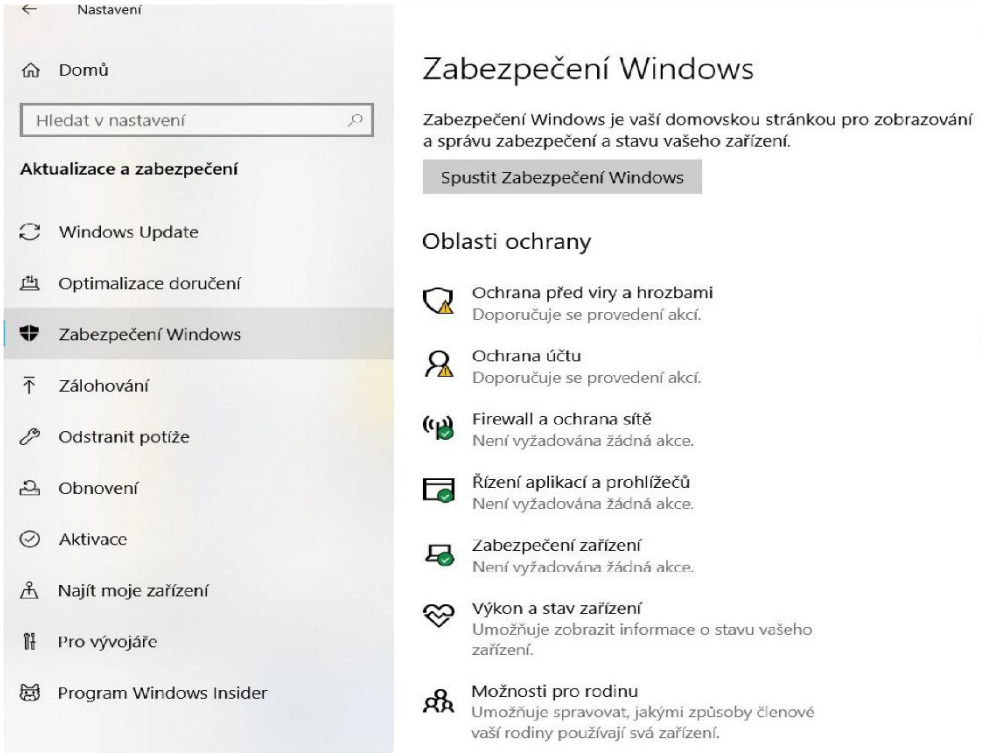
Obr. 39 - Windows Update



Obr. 40 - Windows Update - aktuální systém

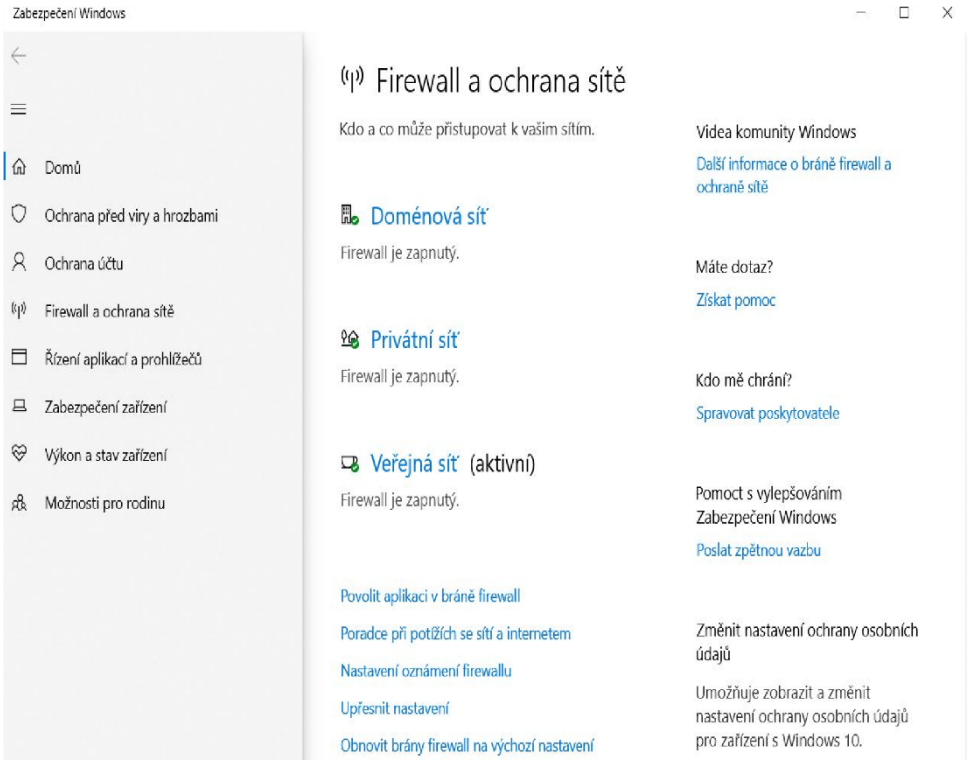
Firewall

Nastavení firewallu se nachází podobně jako aktualizace v *Nastavení → Aktualizace a zabezpečení*. Následně v levém menu zvolte záložku *Zabezpečení Windows*.



Obr. 41 - Zabezpečení Windows

Na stránce vidíte přehled sekce *Oblasti ochrany* vašeho zařízení. Pokud vidíte problém s oblastí *Firewall a ochrana sítě*, klikněte na ni. Zobrazí se detailní informace o konfiguraci firewallu. Můžete zde mimo jiné povolit komunikaci pro novou aplikaci, upřesnit nastavení firewallu nebo upravit oznamování.



Obr. 42 - Firewall a ochrana sítě

Antiviry

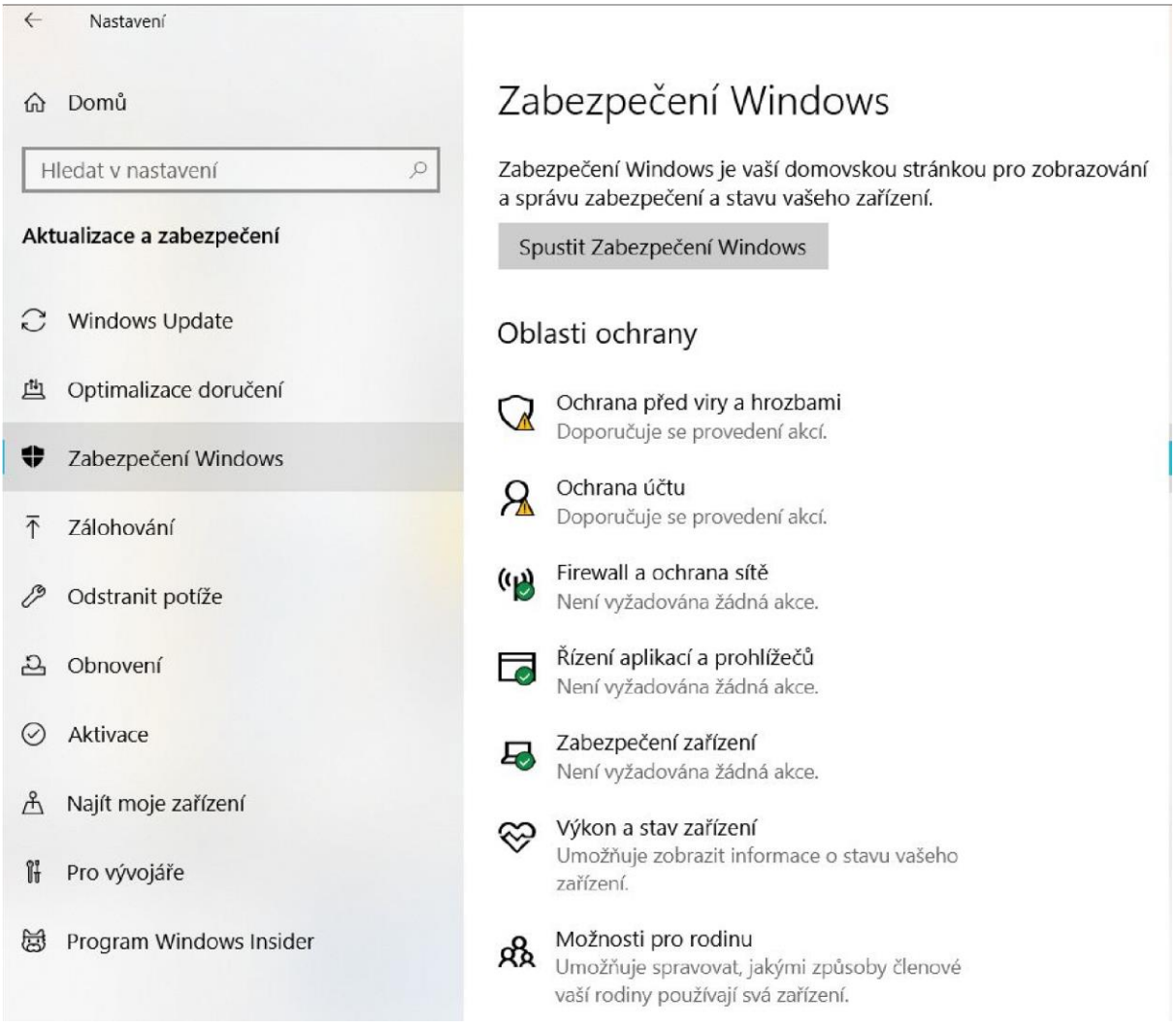
Antivirus je nástroj sloužící k detekci škodlivého kódu, který se do zařízení může dostat mnoha způsoby. K obraně proti infikování zařízení jsou typicky určeny jiné technologie (např. firewall), samotný antivirus tedy není všespásný - je to jakási poslední linie obrany. Často však antivirová řešení v sobě obsahují i další nástroje pro zajištění komplexní bezpečnosti.
Tablety a mobilní telefony jsou častým cílem útočníků a mnohdy obsahují více osobních informací než počítače. Tvrzení, že do mobilu není antivirus třeba, je mýtus.

Výběr antiviru

Antivirové řešení je možné získat zdarma i v placené formě, která mnohdy poskytuje přidanou funkcionalitu. Windows 10 již od instalace obsahuje nástroj Windows Defender.

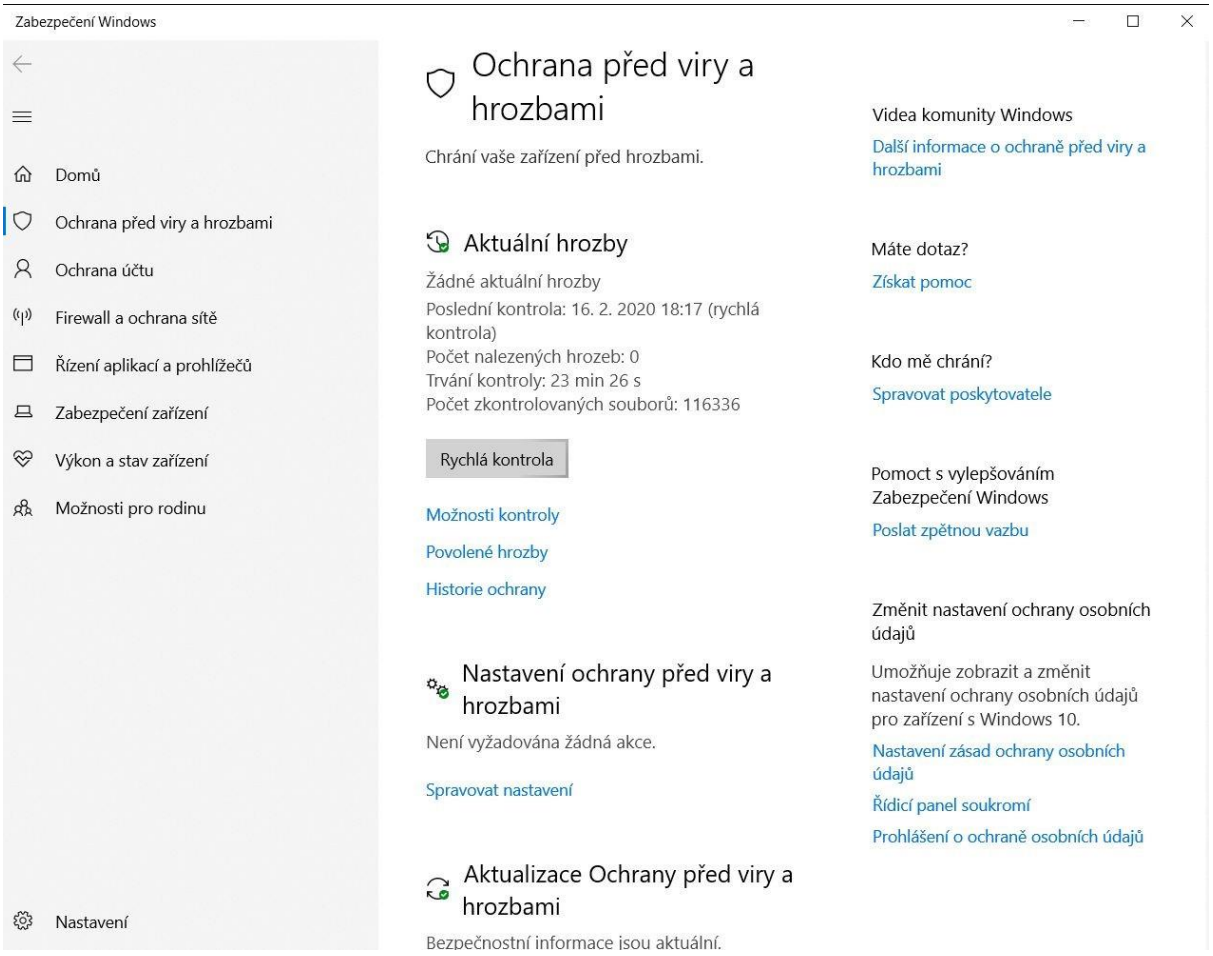
Windows Defender

Nastavení nástroje Windows Defender se obdobně jako firewall nachází v *Nastavení → Aktualizace a zabezpečení → Zabezpečení Windows*. V sekci *Oblasti ochrany* vás nyní zajímá položka *Ochrana před viry a hrozbami*.



Obr. 43 - Zabezpečení Windows

Při rozkliknutí této oblasti ochrany se vám zobrazí nabídka s možnostmi provedení různých typů kontroly, nastavení chování ochrany před hrozbami, historií incidentů a aktualizaci bezpečnostních informací.



Obr. 44 - Ochrana před viry a hrozbami

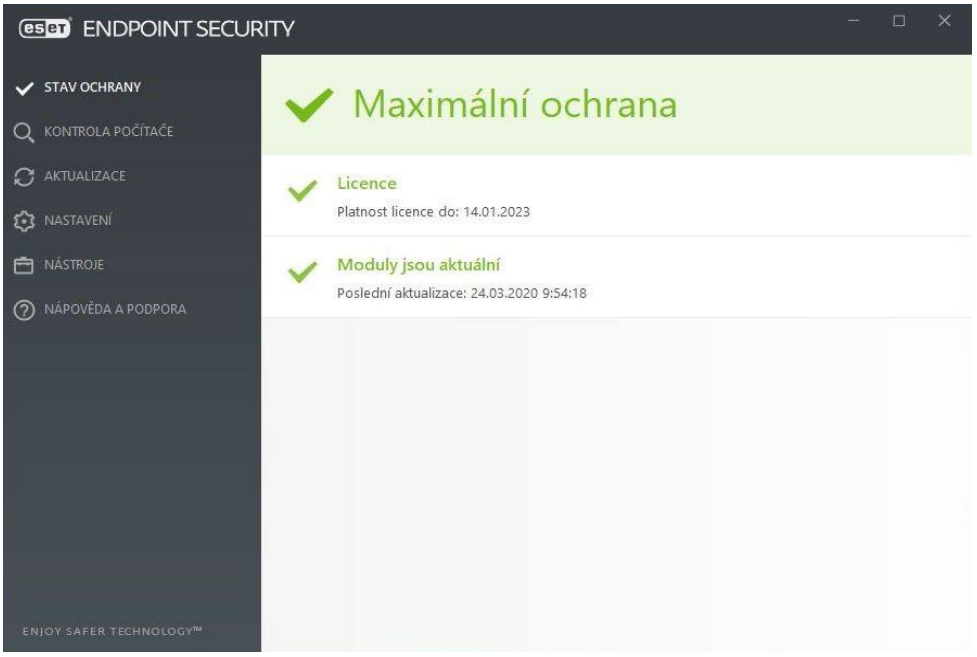
ESET

Licence pro provoz antivirového softwaru ESET skýtá mnoho výhod:

- pomáháte s kolektivní bezpečností - šířená nákaza bude rychleji detekována,
- jste lépe chráněni proti phishingu - rizikové stránky a přílohy budou bezpečnostním týmem blokovány,
- můžete chránit své počítače a mobilní zařízení,
- jsou podporovány nejpoužívanější operační systémy (Windows, Linux, MacOS, Android)
- správcovský přístup na zařízení je zakázán politikami a není tedy možný.

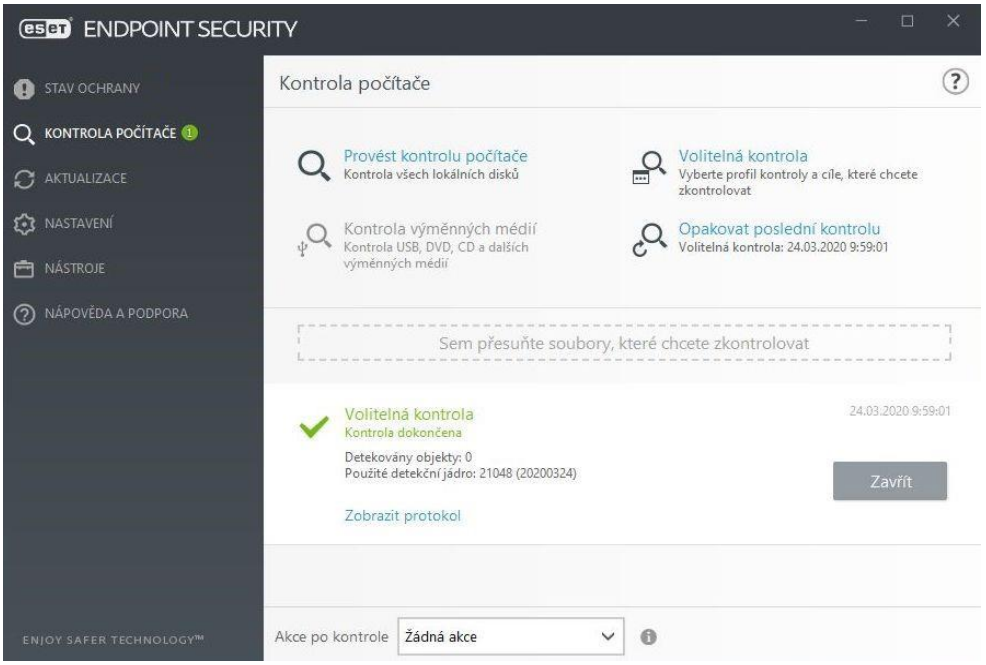
Ovládání antiviru

Po instalaci se v *Oznamovací oblasti* (na liště vpravo) objeví ikona aplikace ESET. Kliknutím na ni se vám zobrazí ovládací rozhraní. První záložka *Stav ochrany* obsahuje informace o tom, zda je váš systém dobře zabezpečen.



Obr. 45 - ESET - stav ochrany

Ze záložky kontrola počítače můžete spustit kontrolu vašeho počítače manuálně. Můžete si vybrat mezi kompletní kontrolou všech disků, volitelnou kontrolou (konkrétní složky), kontrolou výměnných médií (flash disky) nebo nahráním konkrétních souborů ke kontrole. Po ukončení testu se vám v této záložce rovněž zobrazí výsledek.



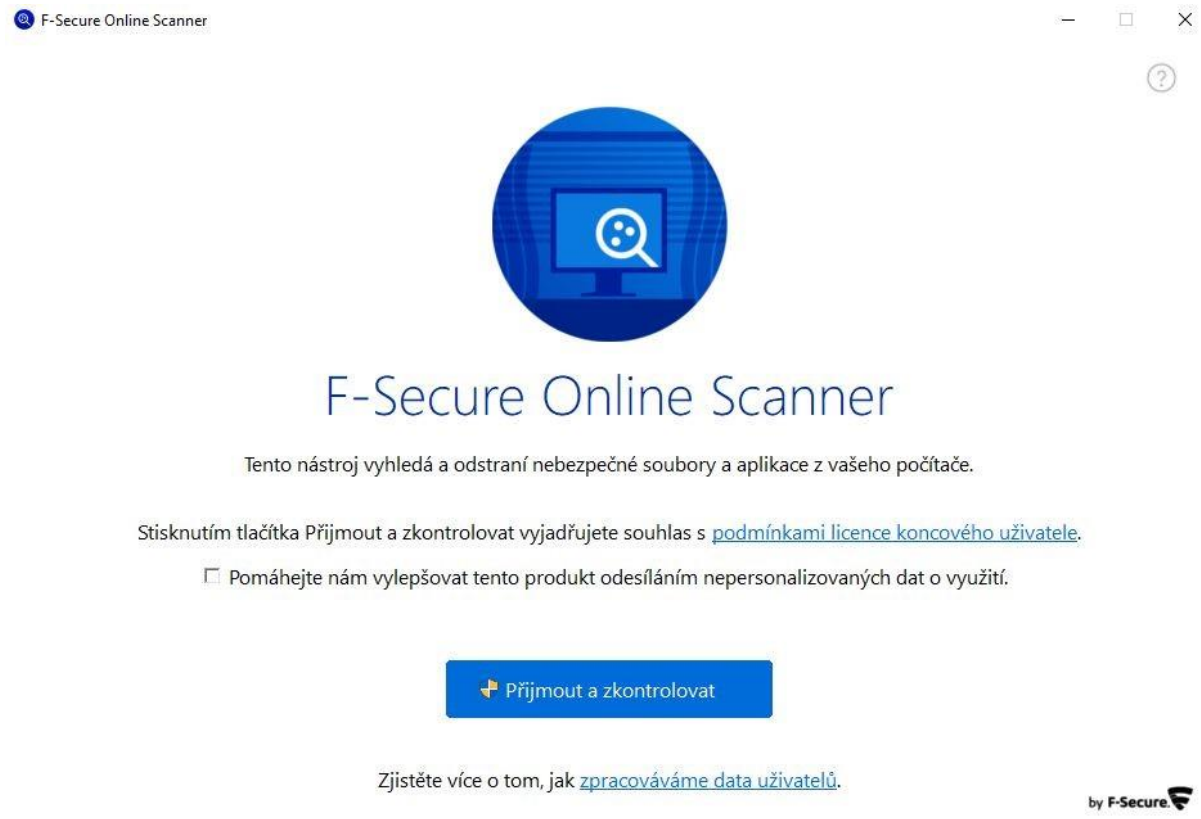
Obr. 46 - ESET - kontrola počítače

Online scannery

Čas od času je vhodné provést kontrolu (scan) zařízení jiným antivirem. Lze tak odhalit hrozby, které instalovaný antivirus neodhalil, a mnohdy lze takto detekovat i případ, kdy byl zavirován samotný antivirus.
Neinstalujte však na jedno zařízení více antivirů, mohou se dostat do vzájemného konfliktu a došlo by k znefunkčnění zařízení. Pro tento účel existují tzv. online scannery. Zde si ukážeme nástroj F-Secure Online Scanner.

Některé z dostupných online scannerů: https://www.eset.com/cz/online-scanner/
https://www.f-secure.com/en/home/free-tools/online-scanner
https://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/online_virus_scan.aspx
https://www.bitdefender.com/toolbox/

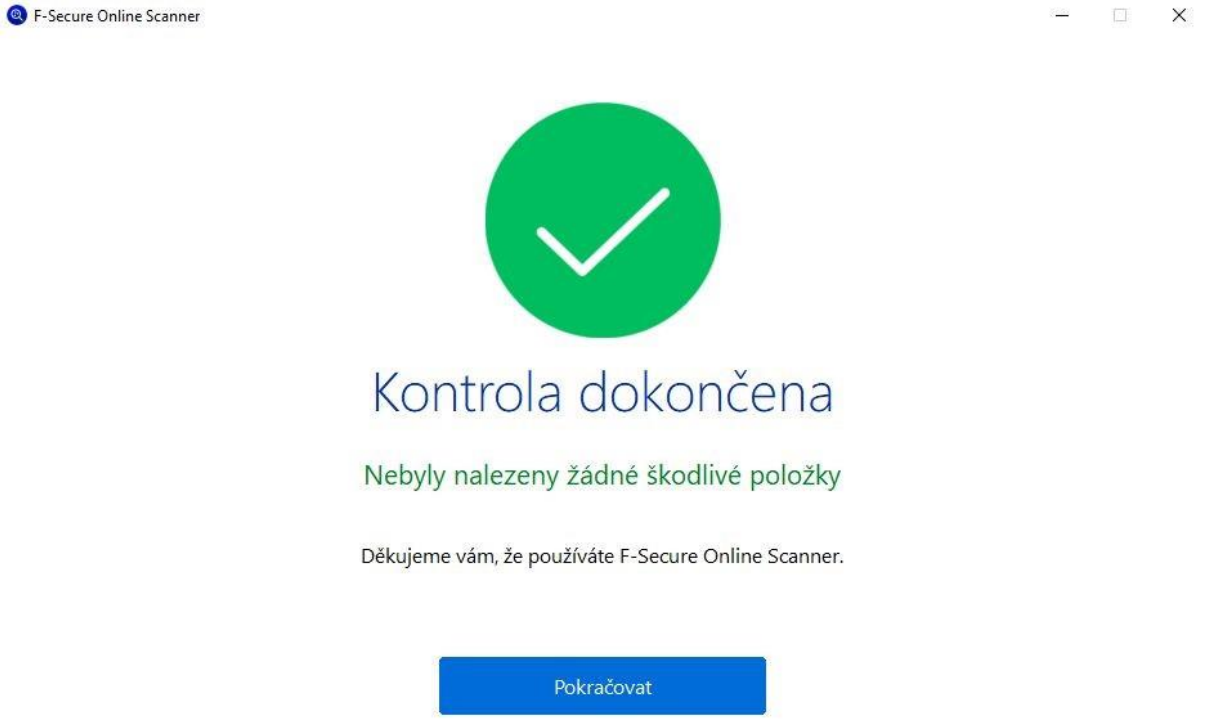
Použití online scanneru je velmi jednoduché. Jednoduše jej spustíte.



Obr. 47 - Průvodce F-Secure Online Scanner

Některé produkty rovněž umožňují výběr druhu kontroly (celý počítač, typicky rizikové části, vlastní kontrola) nebo odstranit aplikace ne vyloženě škodlivé, ale pouze nežádoucí. F-Secure Online Scanner je plně autonomní.

Obr. 48 - F-Secure Online Scanner - průběh scanu



Obr. 49 - Konec scanu

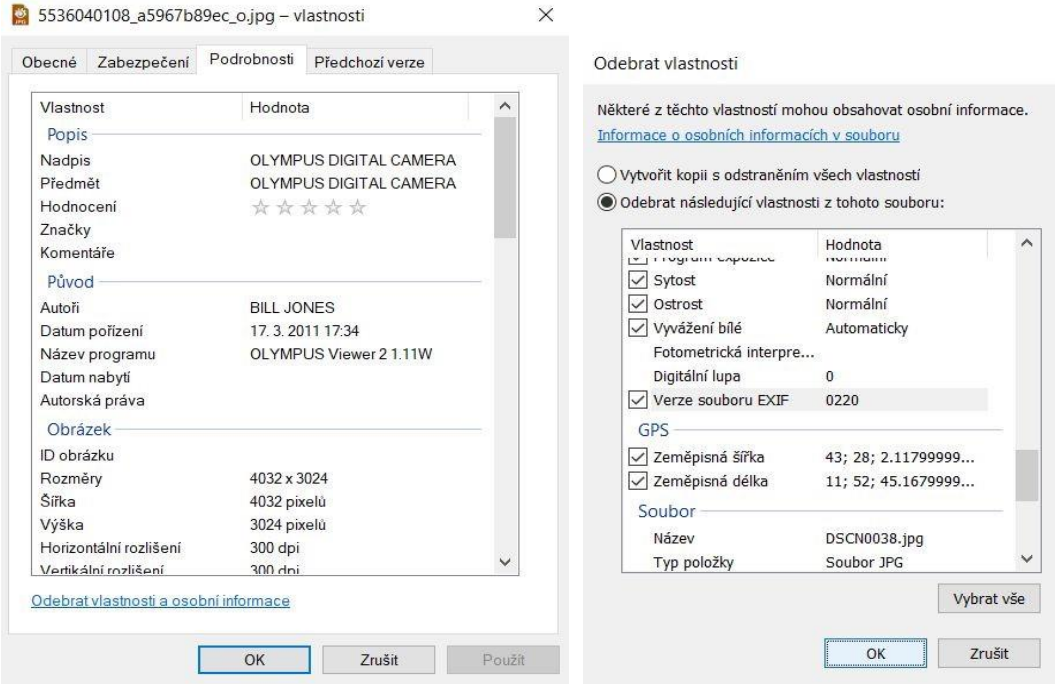
VPN klient

Můžete se dostat do situace, kdy budete nuceni připojit se do sítě, které zcela nedůvěřujete, například na Wi-Fi v kavárně. Tato síť technicky může nahrazovat webové stránky, které navštěvujete, stránkami podvodnými. Rovněž se může stát, že útočník sedící poblíž vytvoří vlastní Wi-Fi síť se stejným názvem a bude doufat, že se k němu někdo omylem připojí. Pokud není Wi-Fi zabezpečená nebo se pro ni používá jedno společné heslo, může se kdokoliv podívat na vaši internetovou komunikaci (šifrovaný provoz, např. přístup na web přes zabezpečený protokol https, ale zůstává uchráněn).
V takových případech je vhodné využít VPN. VPN si lze představit jako tunel, přes který budou chodit všechna vaše data zašifrovaně, a tedy bezpečně přímo z vašeho zařízení až k druhému konci VPN tunelu, kterému důvěřujete (např. do vaší domácí sítě). Zaměstnanci škol mohou využít VPN službu pro takové připojení do své školní sítě.

Anonymizace dat

Soubory, které vytváříte, často obsahují tzv. metadata - informace popisující vlastnosti těchto souborů. Sdílení některých informací může být nežádoucí - jedná se například o informace o vašem uživatelském účtu, datum a čas pořízení fotografie nebo dokonce GPS souřadnice. Systém Windows poskytuje jednoduchý způsob, jak většinu takových informací ze souborů odstranit.

Metadata souboru zobrazíte tak, že na něj kliknete pravým tlačítkem myši, zvolíte možnost *Vlastnosti* a následně si zobrazíte kartu *Podrobnosti*. Pro odstranění metadat v dalším kroku klikněte na *Odebrat vlastnosti a osobní informace* a vyberte, zda se má soubor upravit přímo nebo má být vytvořena jeho kopie a také které vlastnosti mají být odebrány.



Obr. 54, 55 - vlastnosti souboru, odebrání vlastností