

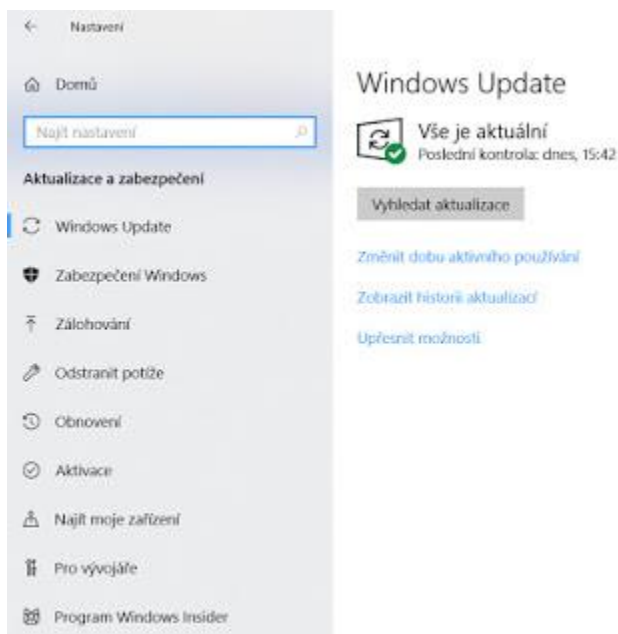
10 pravidel pro bezpečnější IT ve škole

1. Aktualizujte

Pravidelné aktualizace jakéhokoliv SW zajišťují jeho bezproblémový chod a bezpečnosti. Naprostá většina útoků, které se v historii IT stala byla pouhým využitím zranitelností, na které ale v době útoku již existovaly aktualizace a záplaty. Proto je důležité si stanovit plán aktualizací operačního systému a dalších aplikací, které ve škole používáte a ten dodržovat.

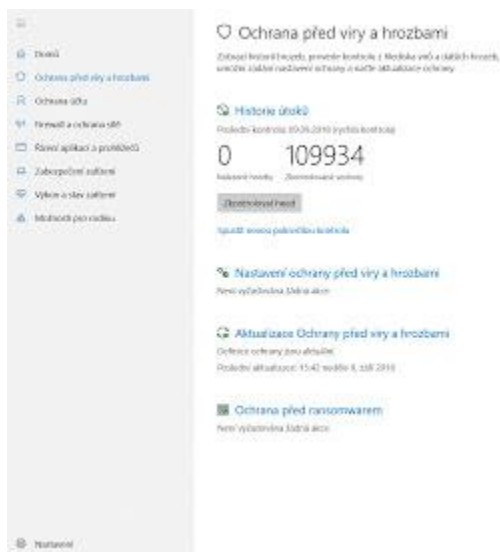
Velká škola si pomocí skupinových politik může nastavit, kdy a jaké instalace se budou stahovat a aktualizovat a přes roli Windows Server Update Services na Windows Serveru si vytvořit lokální aktualizací server, který ušetří mnoho zbytečně stažených dat.

I menší školy ale takové možnosti mají a to přímo v Nastavení systému Windows 10. Zde si mohou nastavit tzv. Dobu aktivního používání, během které nebude docházet k restartování počítače z důvodu instalace aktualizací. A co se týče množství stažených dat? Je možné využít funkci Optimalizace doručení, díky které si počítače v síti budou sdílet aktualizace mezi sebou a nebudou je stahovat každý zvlášť z internetu.



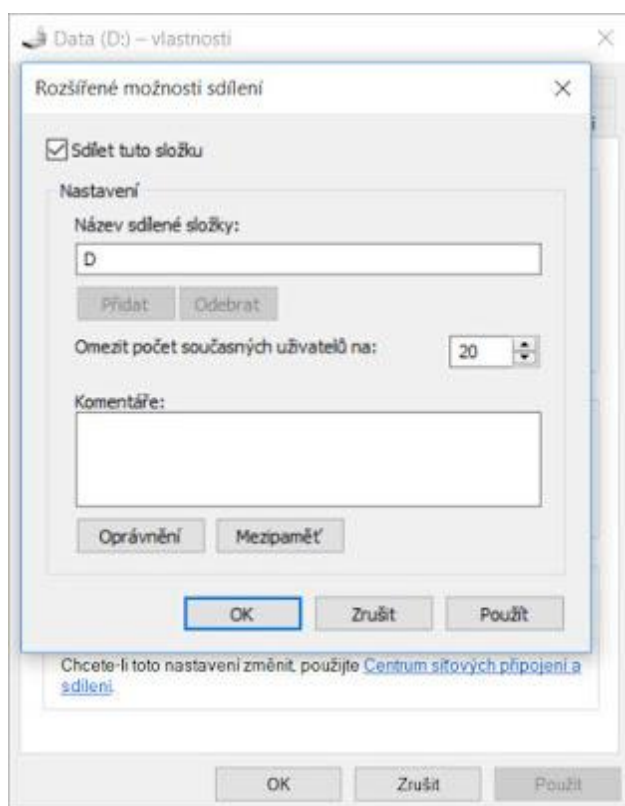
2. Chraňte se

Mít součástí počítačů balík bezpečnostního řešení, který Vás ochrání před nebezpečnými hrozbami internetu je dnes základ. A víte, že jeden takový je již součástí Windows 10? Jmenuje se Windows Defender a obsahuje v sobě ochranu proti virům, spywaru, malwaru a dokonce i ransomwaru. To je ten škodlivý program, který Vám zašifruje pevný disk počítače a požaduje zaplacení výkupného. Navíc v sobě Windows Defender obsahuje i cloudovou ochranu, která Vás ohromnou výpočetní silou datových center ochrání i proti dosud neznámým škodlivým aplikacím.



3. Omezte přístup

Stejně jako od všech místností ve škole nemají všichni klíče, tak i v IT infrastruktuře školy by neměl mít každý přístup všude. Nastavte si tedy taková oprávnění na jednotlivé počítače, složky a soubory, aby k nim mohl přistupovat jen ten uživatel, který to opravdu potřebuje. Přístupy můžete nastavovat jak pro lokální úložiště, tak i pro ty cloudová, jako je OneDrive v rámci Office 365.



4. Ověřujte se

To, že při přístupu k různým službám potřebujete heslo, je asi jasné. Co když ale někdo Vaše heslo zjistí nebo uhodne a přistupuje k Vaším e-mailů, školní matrice a dalším službám a vy o tom nevíte? Jak by ho mohl zjistit? No třeba žáci v první lavici před katedrou vidí velice často celou klávesnici učitele. Zabránit takovému zneužití lze poměrně snadno, stačí si zapnout například v Office 365 dvoufaktorové ověřování, při kterém budete muset ještě zadat ověřovací kód z SMSky nebo autorizační aplikace. Ihned se tak třeba dozvíte, když se někdo snaží přihlásit s vašimi údaji a vy o tom nevíte.

5. Nepřeposílejte.

Alespoň ne automaticky. Mnoho „odpůrců“ nových služeb z řad pedagogického sboru to řeší tak, že si zapne automatické přeposílání na své soukromě adresy. Neuvědomuje si tím však to, že se jedná o automatické vynášení školních dat do soukromého prostředí. Opět. např. ve službě Office 365 máte možnost nastavení automatického přeposílání zcela vypnout.



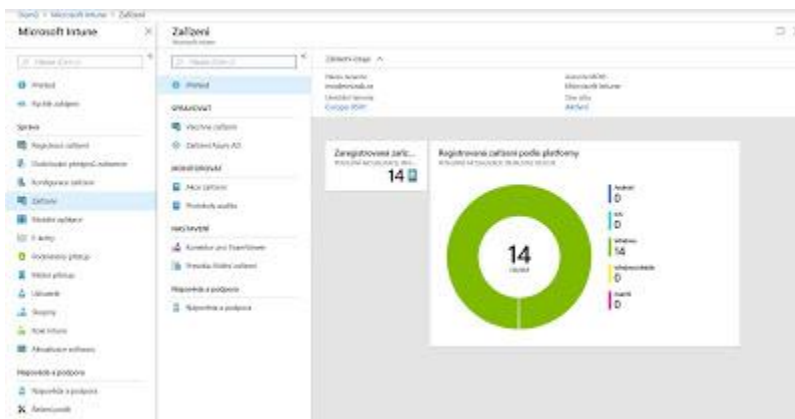
6. Vzdělávejte

Nastavit si IT prostředí tak, aby bylo bezpečné, je relativně snadné, problémem ale poměrně často bývají uživatelé. Co s nimi? Udělat z nich poučené uživatele. Dělejte pro ně pravidelná školení, informujte je o aktuálních hrozbách internetu, ukazujte jim praktické ukázky bezpečnostních incidentů. Součástí služby Office 365 je i kompletní vzdělávací portál, který je o některých takových hrozbách může poučit také. Mezi další vzdělávací aktivity patří ty co spadají pod Microsoft pro školství jako jsou Roadshow pro školy, DemoDays, Večerní univerzity, Letní škola moderních učitelů a mnoho dalších.



7. Kontrolujte

Pokud máte na starosti bezpečnost IT prostředí ve škole, ke potřeba mít přehled a kontrolu opravdu o každém zařízení. Ne pouze tedy o zařízení, které jsou majetkem školy, ale i o těch, které přistupují do školní pošty nebo úložiště, což mohou být i mobilní telefony učitelů. Je to věc, kterou mnoho škol neřeší, přitom je to v případě ztráty telefonu poměrně velká bezpečnostní hrozba. Pusťte tedy do školního mailu jen ty zařízení, která jsou např. šifrovaná a mají nastavený šestimístný PIN. To umí zajistit služba Office 365 a Intune, díky které můžete mít přehled opravdu o všech zařízeních od těch s operačním systémem Windows, přes iOS a MacOS až po Android.

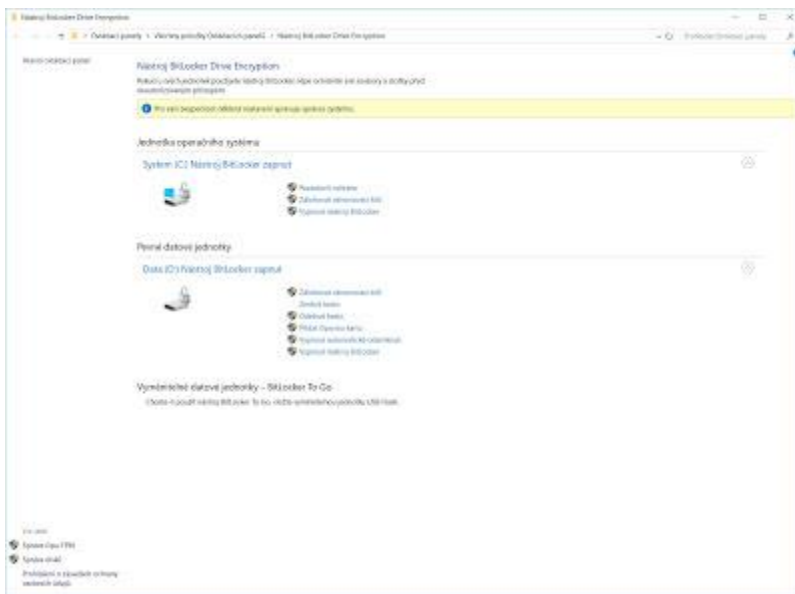


8. Šifrujte

Při ztrátě nebo odcizení notebooku se dnes již ve většině případech neřeší jeho cena, ale to, jaká data na něm byla a jestli je někdo může zneužít. Tomu nepovolanému, kterému se dostane notebook do ruky mnohdy stačí vyndat pevný disk z notebooku a vložit do externího boxu, který připojí k počítači. V tu chvíli má k dispozici víceméně celý obsah disku včetně všech dat.

Tomu zabrání právě šifrování, které zaručí, že se takový disk stane v jiném počítači nečitelný. Ve Windows 10 pro to slouží funkce nazvaná BitLocker. Pro její využití je potřeba mít v počítači TPM (Trusted Platform Module) čip, většina novějších notebooků je má a před zapnutím BitLockeru se provádí i samotná kontrola jeho přítomnosti.

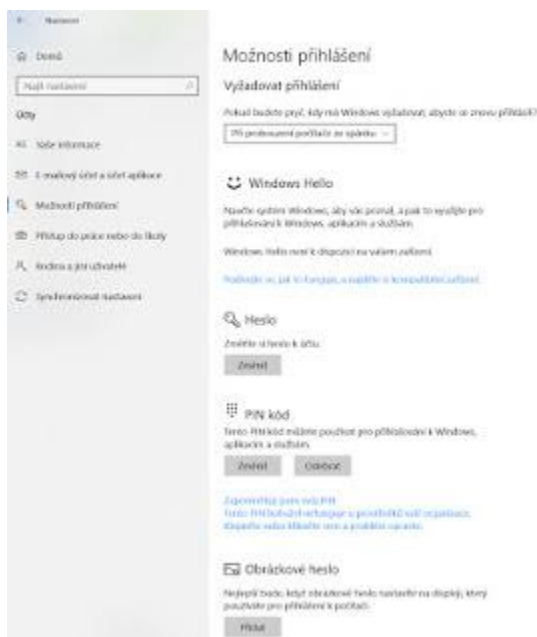
Nezapomeňte, že je potřeba šifrovat i externí disky a USB flash disk. I to BitLocker umí, takže i ztracená flashka nebude znamenat ohrožení školní dat.



9. Zaheslujte

Pro každou službu, ve které je potřeba ověření, je zapotřebí mít uživatelské jméno a heslo. Říká se, že nejlepší heslo je to, které si nepamatujete. Nicméně s ohledem na praktičnost je vhodné zvolit zlatou

střední cestu, tedy např. heslo, které má minimálně 8 znaků, malá a velká písmena, neobsahuje žádné známé slovo a není nijak ve spojitosti s Vámi (rodné číslo, rodné příjmení, telefonní číslo apod.).



10. Zálohujte

Žádný systém nelze asi 100% označit na „neprůstřelný“ a proto je potřeba myslet i na zadní vrátka v podobě záloh. Zálohujte vše, co považujete za důležité a zálohujte pravidelně, nejlépe automatizovaně tak, abyste nemuseli na zálohování vůbec myslet. A kromě zálohování si ale čas od času vyzkoušejte obnovu takto zálohovaných dat, ať v případě reálné potřeby obnovy nejste nepříjemně překvapeni tím, že to možná nejde tak, jak jste si představovali. Pro zálohování Vašich dat můžete využít například úložiště OneDrive, na které se veškeré Vaše soubory a změny, které v nich provedete, uloží automaticky. A jako bonus navíc, OneDrive má zabudovanou ochranu i proti aktuálně největší bezpečnostní hrozbě, ransomwaru.

