Doporučená bezpečnostní nastavení pro macOS

Návod / macOS ■ Ivan Malík

Bezpečnost operačních systémů je často diskutovaným tématem dnešní doby. Ve světě se každou minutu generují neuvěřitelná kvanta dat a podstatná část z nich je umístěna na počítačích uživatelů. Proto je nutné aplikovat politiku zabezpečení, a zamezit tak potencionálnímu úniku těchto dat. V době covidové pandemie to platí dvojnásob. Na internetu se objevují různé návody, jak nejlépe zabezpečit svůj Mac. Jde často o kusé a neúplné informace. To bylo důvodem pro sepsání tohoto článku.

Je potřeba mít na paměti, že se jedná o restriktivní nastavení. Je možné, že nastavením parametrů přijdete o nějakou funkcionalitu, na kterou jste zvyklí. Proto postupujte s rozmyslem a nejprve se ujistěte, že rozumíte tomu, co nastavujete, a že jednotlivá doporučení jsou vhodná i pro vás. V případě, že si nejste jisti, konzultujte vše s vaším oddělením IT.

Doporučené nastavení se vztahuje k aktuálnímu operačnímu systému macOS 10.15 Catalina. Lze jej však (s drobnými úpravami) aplikovat i na nižší nebo vyšší verze operačních systémů macOS.

AKTUALIZACE OPERAČNÍHO SYSTÉMU

Předpokladem správného zabezpečení počítače je aktuálně podporovaný systém. Podporované operační systémy se počítají podle vzorce N – 2, kde N je aktuální verze. V tuto chvíli je to Catalina, Mojave a High Sierra. Ostatní jsou mimo podporu a bezpečnostní aktualizace již nedostávají.

Samostatná část jsou aktualizace systému. Jejich nastavení se provádí v **Předvolbách systému – Aktualizace softwaru – Pokročilé...** a zahrnuje tato doporučená nastavení:

- Povolte funkci **Vyhledávat aktualizace**.
- Povolte funkci **Instalovat aktualizace macOS**.
- Povolte funkci **Instalovat aktualizace aplikací z App Storu**.
- Povolte funkci **Instalovat systémové soubory a bezpečnostní aktualizace**.

NASTAVENÍ SYSTÉMU

Nyní máte aktuální systém. To ale neznamená, že jej máte správně nastavený. Výchozí nastavení počítá s větší tolerancí ohledně bezpečnosti, a pokud tento stav nezměníte, může být počítač napaden útočníkem. Proto je vhodné tyto funkce systému vypnout.

Následující kapitola rozebírá jednotlivá nastavení podle jejich pořadí v Předvolbách systému. Ty najdete v levém horním rohu obrazovky pod ikonou Applu. Je velmi pravděpodobné, že pro změnu některých nastavení budete potřebovat znát heslo správce. Tyto změny povolíte kliknutím na ikonu zámku v levé spodní části okna.

PLOCHA A SPOŘIČ

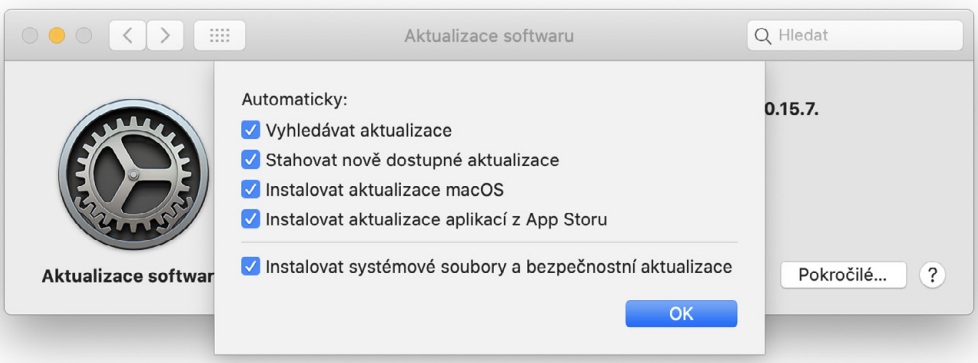
Interval pro spuštění spořiče obrazovky během nečinnosti by neměl být vyšší než 20 minut, proto nastavte volbu **Nastavit po** na hodnotu maximálně do 20 minut. Pomocí nabídky **Aktivní rohy...** si nastavte aktivní roh na **Zamknout obrazovku** nebo **Spustit spořič obrazovky**.

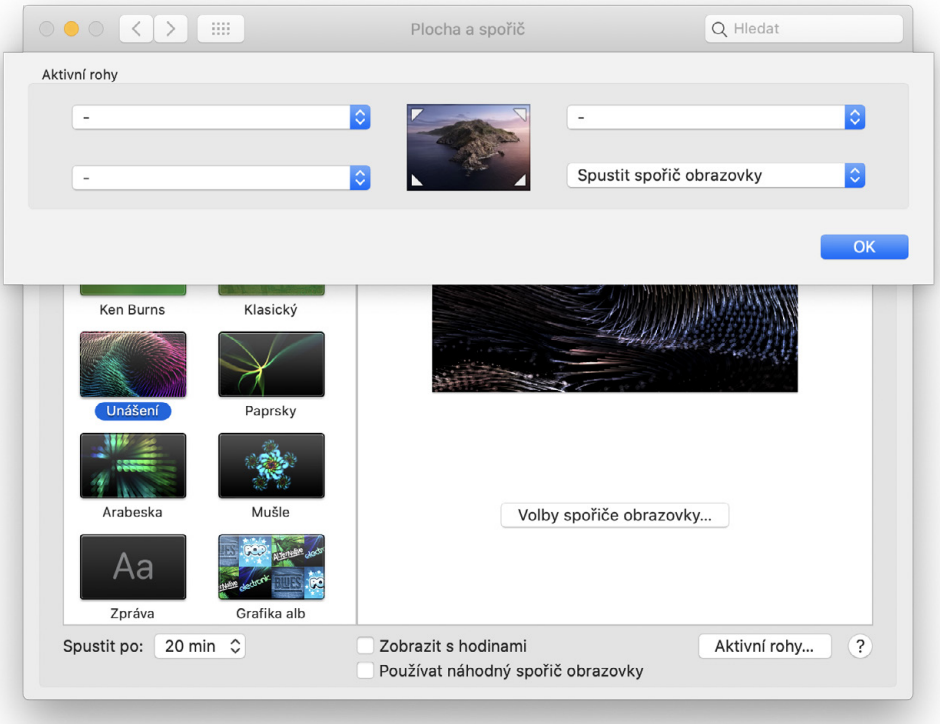
INTERNETOVÉ ÚČTY

V nastavení internetových účtů odstraňte všechny nepoužívané účty a nastavte váš primární účet iCloudu následujícím způsobem:

- Vypněte služby iCloudu, které nepoužíváte.
- Vypněte funkci **iCloud Drive – Volby... – Plocha a složka Dokumenty**.

Zde prosím o vyšší opatrnost – nejdříve si zkontrolujte, že máte dostatečnou kapacitu disku





a po vypnutí této funkce se ujistěte, že víte, kde jsou dokumenty umístěny. Poté je přesuňte na lokální plochu (**~/Plocha**) a do lokální složky Dokumenty (**~/Dokumenty**).

Současně s tím si projděte nastavení svého účtu Apple ID. Zkontrolujte, že máte zapnuto dvoufaktorové ověřování – oddíl **TWO-FACTOR AUTHENTICATION** by měl být ve stavu **On**. V oddílu **APP-SPECIFIC PASSWORDS** – odkaz View History a v oddílu **APPS & WEBSITES USING APPLE ID** si zkontrolujte přístup aplikací a nepoužívané položky odstraňte.

UŽIVATELÉ A SKUPINY

Zkontrolujte seznam uživatelů a odstraňte ty, kteří nemají mít k počítači přístup. Pokud vám to vyhovuje, vyberte si v nastavení **Volby přihlášení** raději zobrazování přihlašovacího okna jako **Jméno a heslo** místo **Seznam uživatelů** a zakažte **Zobrazování nápovědy pro heslo**. Po splnění těchto úkolů proveďte ještě následující kroky:

- **Vypněte účet Host** a podružnou funkci sdílení **Povolit hostům připojení ke sdíleným složkám**. Tento účet je automaticky povolen například, pokud uživatel používá funkci **Najít**.
- Odstraňte z disku uživatelskou složku **/Uživatelé/Host**.
- Nastavte si komplexní heslo a ověřte jeho minimální délku. Komplexní hesla by měla obsahovat kombinaci velkých a malých písmen, čísla a jednoho speciálního znaku a měla by být alespoň 8 znaků dlouhá.
- Pro přihlášení do systému použijte unikátní heslo, které jinde nepoužíváte.
- Přepněte volbu **Automatické přihlašování** na **Vypnuto**.
- Vypněte volbu **Rychlé přepínání uživatelů**.

ZABEZPEČENÍ A SOUKROMÍ

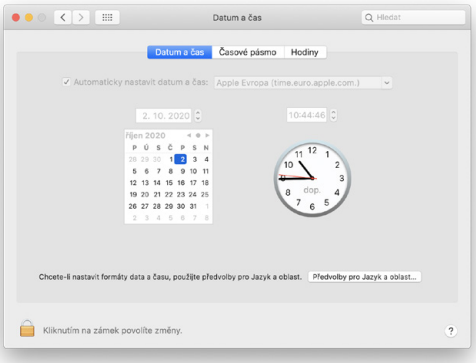
Většina nastavení zabezpečení systému se skrývá v **Předvolbách systému – Zabezpečení a soukromí**. Doporučuji pečlivě projít všechny záložky a nastavit minimum podle následujících pokynů.

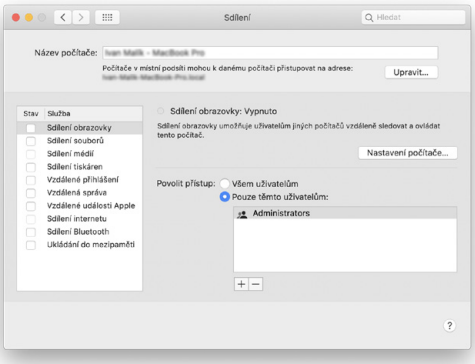
ZÁLOŽKA OBECNÉ

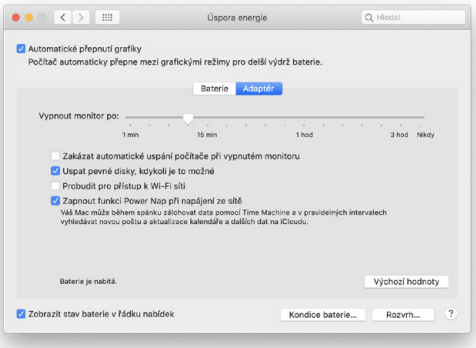
- Nastavte službu Požadovat heslo bezprostředně po uspání nebo spuštění spořiče obrazovky.
- Nastavte si zprávu na uzamčené obrazovce.
- Nastavte funkci Povolit aplikace stažené: na „z App Storu a od známých vývojářů“.

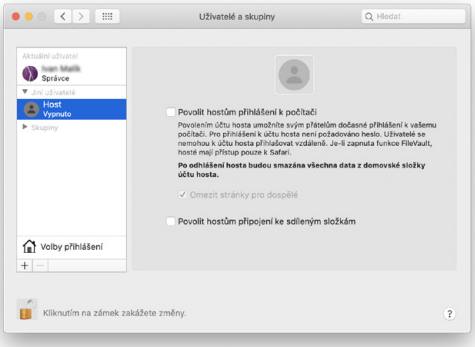
ZÁLOŽKA FILEVAULT

FileVault 2 je technologie, která se stará o šifrování disků a je tak základním stavebním kamenem bezpečnosti dat. Proto je potřeba tuto funkci zapnout.









Klíč zotavení uložte na bezpečné místo. Pokud je počítač spravován řešením MDM, lze k odemčení použít i Klíč organizace.

FileVault 2 používá silné šifrování AES-256 s 128bitovými bloky v režimu XTS a po zapnutí dojde ke snížení výkonu počítače o několik jednotek až desítek procent (obzvlášť u starších počítačů).

ZÁLOŽKA FIREWALL

Velkým omylem (a bohužel i některých „ajťáků“) je představa, že jde o paketový firewall, který umí zahodit paket na základě pravidel. Není to pravda. Jde o tzv. aplikační firewall umožňující identifikovat a vynucovat zásady obsahu specifického pro aplikaci. Dohromady společně fungují tak, že paketový firewall, zahodí paket a aplikační firewall jej již nezpracovává.

Tento aplikační firewall si nejdříve aktivujte, a poté v nabídce **Volby firewallu...** zapněte neviditelný režim a zkontrolujte seznam pravidel.

ZÁLOŽKA SOUKROMÍ

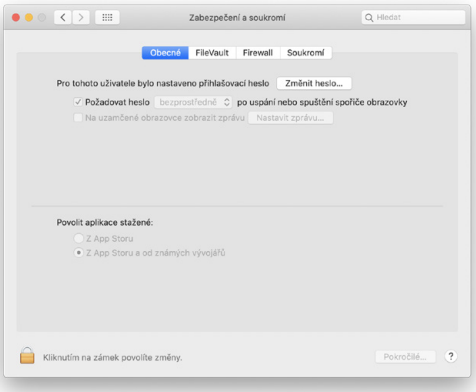
V sekci **Soukromí** povolte polohové služby a ověřte, zda k ní mají přístup pouze důvěryhodné aplikace. Aplikace, které jsou označené generickou ikonou, nejsou v počítači nejspíš nainstalované. Vypněte jejich přístup a ze seznamu budou automaticky odstraněny. V seznamu najděte poslední položku **Systémové služby** a pod nabídkou **Podrobnosti...** ověřte, že máte povolen přístup pro funkci **Najít můj Mac**.

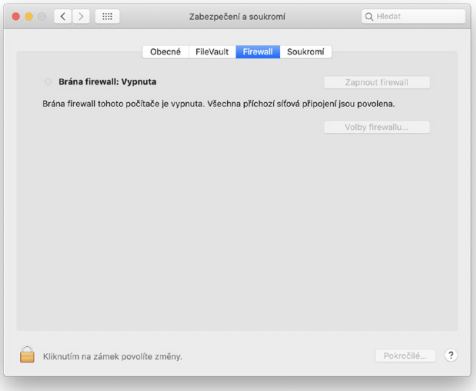
Podobným způsobem projděte další nastavení a ověřte, že k jednotlivým službám mají přístup opět pouze důvěryhodné aplikace. V sekci **Analýza a vylepšování** doporučuji zakázat odesílání dat pomocí funkce **Sdílet data analýzy Macu**, **Vylepšování Siri a diktování** a **Sdílet data analýzy iCloudu**.

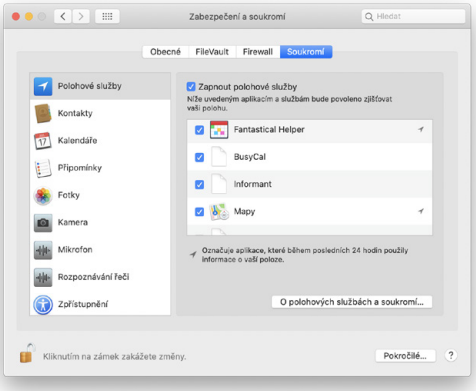
SÍŤ

Velmi opomíjené nastavení systému, které díky různým migracím bobtná a v krajním případě tak může představovat bezpečnostní riziko. Jde především o zbytečná síťová rozhraní a Umístění. Zbytečné položky odstraňte následujícím způsobem:

- V nabídce **Umístění – Upravit umístění** odstraňte stará umístění a používejte pouze ta aktuální.
- V seznamu síťových rozhraní odstraňte zbytečná a nepoužívaná rozhraní. Pod ikonou nastavení najděte volbu **Nastavit pořadí služeb...** a přetažením nastavte správné primární rozhraní.
- Pro rozhraní Wi-Fi povolte službu **Zobrazit stav Wi-Fi v řádku nabídek**.
- Pro rozhraní Wi-Fi vypněte funkci **Zeptat se na připojení nových sítí**.







- Pokud to je možné, nepoužívejte vlastní nastavení DNS pro Ethernet a rozhraní Wi-Fi (např. **Wi-Fi – Pokročilé... – DNS**).

ÚSPORA ENERGIE

V tomto nastavení se skrývá funkce **Probudit pro přístup k síti Wi-Fi**, jenž umožňuje uživatelům přístup ke sdíleným prostředkům počítače v režimu spánku – ať již sdílené tiskárny nebo playlisty aplikace Hudba. Tuto funkci je vhodné vypnout.

DATUM A ČAS

V dalším kroku se zabýváme poměrně banálním nastavením data a času. Obě proměnné se používají pro zápis a čtení souborů a závisí na nich digitálně podepsané aplikace nebo certifikáty. Pokud je nebudete mít správně nastavené, můžete mít problém např. se spouštěním aplikací, otevíráním webových stránek nebo dokonce nefunkčními certifikáty. Ujistěte se proto, že jste provedli tyto kroky:

- Povolte funkci **Automaticky nastavit datum a čas** a vyberte server NTP, který je k vám geograficky nejblíže.
- Ujistěte se, že nastavení času odpovídá tomu reálnému (s maximální odchylkou v řádu sekund).

Pokud nesouhlasí čas počítače s časem reálným, máte problém se serverem NTP. To je ale úkol pro vašeho správce IT.

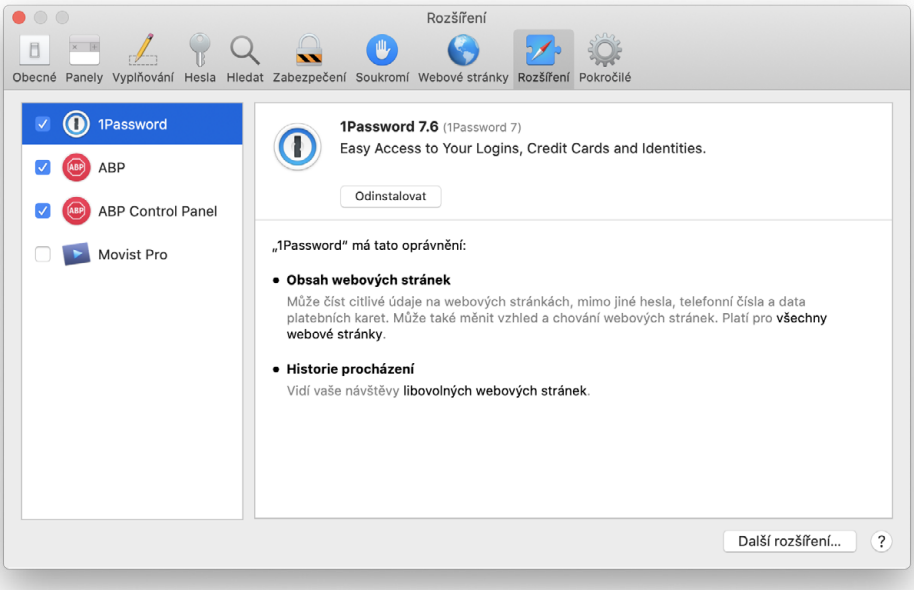
SDÍLENÍ

Opomíjené nastavení, které umožňuje sdílet některé hardwarové a softwarové služby počítače s ostatními uživateli. Toto nastavení je vhodné pro jednodušší workflow nebo jednorázový přístup. Profesionální řešení používají většinou proprietární protokoly. Navíc tyto služby používají IP multicast (v Apple světě označovaný jako Bonjour) a zahlcují tak zbytečně síťový provoz. Proveďte následující kroky:

- Vypněte službu **Sdílení obrazovky**.
- Vypněte službu **Sdílení souborů**.
- Vypněte službu **Sdílení médií**.
- Vypněte službu **Sdílení tiskáren**.
- Vypněte službu **Vzdálené přihlášení**.
- Vypněte službu **Vzdálená správa**.
- Vypněte službu **Vzdálené události Apple**.
- Vypněte službu **Sdílení internetu**.
- Vypněte službu **Sdílení Bluetooth**.
- Vypněte službu **Ukládání do mezipaměti**.

TIME MACHINE

Zálohování dat je bezpochyby velmi důležité.



Pomůže vám dostat se k datům i v takových případech, kdy bude počítač odcizen nebo úložiště havaruje. Data, která jsou mimo počítač, jsou ale snadným terčem a lze je snadno zcizit. Proto je potřeba zkontrolovat, že jsou zálohy Time Machine zašifrovány a že máte bezpečně uložen šifrovací klíč.

Rozmyslete si, které složky nepotřebujete zálohovat. Čím menší je záloha, tím bude zálohování a obnova rychlejší a náročnost na síťový provoz bude nižší. Například složku **/System** není nutné zálohovat.

OSTATNÍ

V **Předvolbách systému** zaměřte ještě svou pozornost na tyto dvě:

- V předvolbách pro Siri vypněte funkci **Požadavky na Siri**.
- Na počítačích, které nejsou spravovány řešením MDM, používejte předvolbu **Čas u obrazovky** a vhodným způsobem omezte přístup jednotlivým aplikacím.

PŘÍSTUP A AUTENTIZACE

Přístup a autentizace jsou další dvě kritické oblasti zabezpečení a jejich nerespektování může vést k převzetí kontroly útočníkem. Především v případě, kdy počítač není spravován řešením MDM. Doporučené nastavení zahrnuje tyto kroky:

- V aplikaci **Terminal** ověřte příkazem **csrutil status**, že je povolen SIP. Pokud je odpověď systému **System Integrity Protection status: disabled**, restartujte počítač a v **Recovery** režimu zadejte v aplikaci **Terminal** příkaz **csrutil enable** a **reboot**.
- Používejte bezpečnostní a biometrické prvky konkrétního zařízení (například Touch ID nebo přihlašování pomocí Apple Watch).
- Pro přístup k **Předvolbám systému** vyžadujte heslo správce.
- Nepovolujte v aplikaci **Adresářová služba uživatele root**.
- Naučte se pro rozdílné účely vytvářet samostatné klíčenky.

OSTATNÍ NASTAVENÍ

Další doporučená nastavení se týkají ostatních částí systému a zahrnují tyto kroky:

- Ujistěte se, že všechny uživatelské oddíly jsou šifrovány (**Disková utilita – Oddíl – Informace – Zašifrovaný – Ano / Ne**).
- Vypněte funkci automatického otevírání „bezpečných" souborů v aplikaci Safari (**Safari – Předvolby – Obecné – Bezpečné soubory po stažení otvírat**).
- Zkontrolujte rozšíření Safari s globálním přístupem, a pokud je nepotřebujete, odstraňte je (**Safari – Předvolby – Rozšíření**).
- Viditelnost AirDrop změňte na volbu **Pouze kontakty**.
- A vždy, když odcházíte od počítače, jej uzamkněte pomocí aktivního rohu.

Pokud jste dočetli až sem, máte bezpečnostní minimum úspěšně splněno. Cílem bylo nastavit systém z uživatelského rozhraní tak, aby splňoval základní bezpečnostní parametry. A to se nám právě úspěšně podařilo.