# Bezpečná zařízení

Počítače, telefony, tablety, chytré hodinky, robotické vysavače nebo na síť připojené centrifugy v laboratoři. To všechno (a mnoho dalšího) jsou zařízení, která mohou být využita k útoku na naši kyberbezpečnost. Musíme je proto chránit, a to jak s ohledem na jejich fyzickou ochranu, tak s důrazem na jejich programové vybavení a data, která do nich ukládáme. V pátém modulu se společně zaměříme na obecná pravidla ochrany zařízení, promluvíme si o využití šifrování a na závěr se plynule dostaneme i k tématu potřeby zálohování dat a souborů z našich zařízení.

# Obecná pravidla práce se zařízeními

## Zamykat, zamykat, zamykat

Kdo si nezamyká počítač při odchodu z kanceláře, a ještě si k tomu nechává třeba v prohlížeči přihlášený Facebook, ten si přímo říká o klasický žert, kdy kolegové na sociální síť pod jeho jménem nasdílí nevhodné komentáře. To je ale ve finále to nejmenší, co se může stát. Zařízení je prostě v době, kdy ho nepoužíváme, třeba zamykat – jinak na něm může kdokoliv provádět cokoliv a celé naše nastavování silných hesel anebo 2FA (viz modul 2) je nám úplně k ničemu. Potřeba fyzické ochrany se samozřejmě týká i telefonů a dalších zařízení.

|  |
| --- |
| **Vyzkoušejte si...** rychle uzamknout svůj počítač s Windows. Stiskněte kombinaci kláves *Ctrl + Alt + Delete* a vyberte možnost *Uzamknout*. Ještě rychlejší je využít klávesové zkratky pomocí současného stisknutí klávesy *Windows* a písmene *L*. To při odchodu od počítače zvládnete během vteřiny. Na Macu můžeme využít klávesové zkratky *Control + Command + Q* a na zařízení s Linuxem většinou funguje kombinace *Ctrl + Alt + L*. |

## Moje je moje, tvoje je tvoje

Moje pracovní zařízení je moje zařízení a můj účet je můj účet. Potřebujeme zkontrolovat pracovní poštu, ale notebook se nám vybil a k dispozici teď máme jen starší domácí počítač našeho potomka? A máme jistotu, že je jeho zařízení skutečně bezpečné? Nebo takhle: spolužačka na přednášce se nemůže připojit k síti eduroam a poprosí nás, abychom se v jejím zařízení přihlásili na svoje jméno a heslo. Vzpomínáte na techniku sociálního inženýrství nazvanou *pretexting* z modulu 4? Takže s omluvou odmítneme. Moje pracovní zařízení je prostě moje a moje údaje jsou taky moje, nikomu je nepůjčujeme.

## Číst směrnice má smysl

Každá instituce má směrnice, které upravují, co se smí a co se nesmí. Některé směrnice míří přímo na práci s IT a na kyberbezpečnost, je proto vždy rozumné si je nastudovat. <school-specific> Na MUNI je vhodné si nastudovat především směrnice MUNI č. 10/2017 a č. 9/2017. <school-specific>

## Soukromá zařízení v pracovním nasazení

Pokud máme pracovní zařízení, používáme k pracovní agendě vždy přednostně to. Ne vždy ale máme svůj vlastní pracovní telefon nebo notebook, a tak se může stát, že soukromá zařízení využíváme třeba pro psaní pracovních e-mailů nebo proplácení faktur. Pokud tomu tak je, musíme opravdu důsledně dbát všech zásad z ostatních modulů, jako např. volit silná hesla, mít nainstalovaný antivirový program (viz dále) atp. Je to na naši zodpovědnost.

|  |
| --- |
| **Pozor!** Používání zařízení se vždy řídí směrnicemi. <school-specific: propojit s interními směrnicemi> Směrnice MUNI č. 10/2017, článek 3, odstavec 5, o osobních zařízeních říká toto: „Uživatel je oprávněn přistupovat k IT MU i prostřednictvím technického a programového vybavení, sítí a služeb, které do nich nespadají. Zároveň je však povinen zajistit, aby tak nezpůsobil bezpečnostní incident.“ |

## Stojí za to potlačit zvědavost

Na chodbě na okenním parapetu se povaluje opuštěná USB paměť. Nebo v knihovně někdo zapomněl na stole paměťovou SD kartu. Zvědavost nás pálí, často i v představě dobrého skutku, že podle souborů na „flashce“ či na kartě najdeme majitele a jeho ztracenou paměť mu vrátíme. Zvědavost ale musíme potlačit, tento typ útoku se na přirozenou lidskou zvědavost spoléhá – a často úspěšně. K našemu zařízení prostě nepřipojujeme žádná neznámá média, protože nikdy nevíme, co na nich číhá.

## Antivir je stále nutnost

Každý den stahujeme soubory z internetu a otvíráme dokumenty z pošty. Naším zařízením projdou desítky a stovky souborů, které mohou být potenciálně nebezpečné: mohou v sobě ukrývat škodlivý kód. Mít na svém zařízení antivirový program, který dokáže tyto potenciálně nebezpečné soubory identifikovat a zastavit dříve, než napáchají škodu, je jednoznačně potřeba. Antivirový program je také nutné udržovat aktualizovaný, ale o to se většinou postará program sám automaticky.

|  |
| --- |
| **Víte že...** více není vždy lépe? Není dobré na jedno zařízení instalovat více antivirových programů. Ačkoliv se může zdát, že duální ochrana bude efektivnější, dva a více aktivních antivirových programů mohou vést naopak ke kontraproduktivní detekci nebo nedostatečné ochraně. Tématem je také antivirový program na mobilních zařízeních. Obecně ho doporučujeme i zde, zásadnější prevencí je tu však pravidelná aktualizace operačního systému (např. Android) a nainstalovaných aplikací. |

## Aktualizovat, i když nás to zdržuje

Ano, aktualizující se Windows v momentě, kdy to nejméně potřebujeme (třeba když máme za pět minut důležitou poradu), to je skutečně otrava. Ale aktualizace nejsou jen nové funkce a vizuální změny v operačním systému – aktualizace jsou především **reakce na odhalené bezpečností díry**. Automatické aktualizace proto **nikdy nevypínáme** a pokud je nám nabídnuta možnost je odložit, odkládáme je jen ve velmi zásadních případech. Tato pravidla se týkají nejen operačního systému Windows, ale také všech nainstalovaných aplikací a programů a samozřejmě i systému na našem mobilním telefonu nebo tabletu (např. Android).

Většina systémů a aplikací se aktualizuje sama a automaticky (*popřípadě nám existenci aktualizací oznámí a vyzve nás k jejich instalaci*), ale i tak je dobré kontrolovat, že automatické aktualizace probíhají. Pokud zjistíme, že tomu tak není, je vhodné tuto skutečnost hlásit a řešit s IT podporou.

|  |
| --- |
| **Vyzkoušejte si...** některý z mnoha hlídačů aktualizací. Na počítači máme většinou velké množství aplikací a pravidelně sledovat, zda jsou všechny skutečně aktualizovány, může být celkem náročné. Proto existují nástroje, které nás na nové verze programů umí upozornit. Vyzkoušet můžete např. [Avira Software Updater](https://www.avira.com/en/software-updater) (omezená verze zdarma) nebo [SUMo](http://kcsoftwares.com/index.php?sumo) (verze zdarma). |

## Zařízení není jen počítač a telefon

Jak dramaticky roste množství zařízení kolem nás, které jsou připojená k internetu, roste spolu s tím i počet možností, kudy vést útok na naše kyberbezpečí. V době takzvaného ***internetu věcí***, kdy jsou ke globální síti připojeny i naše lednice, žárovky, domácí bezpečností kamery, chytré televize nebo mikroskopy v laboratoři, je třeba mít se na pozoru. Případy, kdy útočníci využili slabého zabezpečení těchto zařízení a například odmrazili ledničku nebo vystrašili obyvatele bytu zhasínáním a rozsvěcením světel v posledních letech přibývá. Většinu rizik lze vyřešit starými dobrými postupy: pevná hesla, pravidelné aktualizace atp. Řešení některých bezpečnostních rizik těchto zařízení je ale mimo možnosti nás jako uživatelů – je ale dobré o rizicích alespoň přemýšlet: co by se mohlo stát, pokud by útočník například získal kontrolu nad mým robotickým vysavačem? Dokážeme si takový scénář představit? Může být reálnější, než se zdá.

## Zařízení není jen robotický vysavač a chytrá žárovka

Počítač, telefon, tablet, chytrá žárovka nebo inteligentní lednička... Nezapomínáme ještě na něco? Ještě jsou tu zařízení, které nedržíme v ruce každý den jako telefon či tablet, ani nejsou tak sexy jako moderní prvky chytré domácnosti nebo chytré vybavení v kanceláři či laboratoři. Jsou to všechny ty krabičky za stolem a pod televizí, které nás propojují s globální komunikační sítí: Wi-Fi, routery, rozbočovače, zesilovače atp. I ty mohou být cílem či prostředníkem útoku. V zaměstnání za nás jejich bezpečnost řeší kyberbezpečnostní tým a IT oddělení, doma se o ně ale musíme většinou postarat sami.

|  |
| --- |
| **Víte že...** byla doba, kdy se dalo z názvu sítě poskytovatele internetu UPC odvodit heslo a během vteřiny se tak připojit i na zabezpečenou domácí WiFi vašeho souseda – a skrze to třeba až do jeho síťového datového úložiště plného soukromých souborů? Dnes už to tak jednoduché není, ale **co vaše domácí heslo na Wi-Fi?** Odpovídá tomu, co jsme si o heslech ukázali v modulu 2? Není čas ho změnit? Prostudujte si návod k vašemu zařízení, kde zjistíte, jak na to. |

## Šifrovat jako na skautském táboře

Raději tedy poněkud sofistikovaněji, než jak se šifruje na skautském táboře. O šifrování už jsme mluvili v modulu 3 o bezpečné komunikaci v souvislosti s takzvaným E2E šifrováním. Zabezpečení komunikace ale není jediná oblast, kde šifrování může pomáhat. Stalo se vám už také někdy, že jste ve veřejném počítači nebo na veřejném místě zapomněli svoji USB paměť? Kdokoliv ji našel, mohl se dostat jednoduše ke všem souborům, které na ní byly uloženy. Doufejme, že to nebyly žádné citlivé dokumenty...

Přitom by stačilo tuto paměť zašifrovat – tak se na šifrování pojďme podívat trochu blíže a podrobněji.

# Šifrování

Když mluvíme o šifrování, myslíme tím většinou nějaký (často velmi složitý) matematický proces, který zajišťuje, že informace, které chceme zabezpečit, budou čitelné pouze pro toho, kdo má klíč k jejich rozšifrování. Šifrování je velmi efektivní metoda a setkáváme se s ním v mnoha různých podobách.

**Šifrování komunikace** – v dnešní době běžně posíláme citlivé informace e-mailem nebo přes komunikační aplikace. V modulu 3 už jsme si ukázali, že zprávy posílané přes internet mohou být za určitých podmínek po cestě přečteny - a že řešením je třeba takzvané E2E (koncové) šifrování. Pokud už si na něj nevzpomínáte, vzhůru zpět do modulu 3!

**Brouzdání po webu** – prohlížení webu není nic jiného než neustálý proud souborů, textů a obrázků mezi námi a počítači v internetu - tzv. servery. Toto posílání se odehrává přes různé protokoly, jedním z nich je i protokol HTTP. Aby bylo zajištěno, že je naše brouzdání webem o něco bezpečnější, využívá se jeho šifrovaná varianta *HTTPS*. Dnes už většina stránek používá HTTPS: tedy umožňuje uživatelům například bezpečné přihlašování do internetového bankovnictví či emailové schránky tak, aby posílané informace nemohl nikdo odposlouchávat cestou po síti.

|  |
| --- |
| **Vyzkoušejte si...** doplněk do prohlížeče [HTTPS Everywhere](https://www.eff.org/https-everywhere)! Některé webové stránky šifrovanou variantu protokolu HTTP nabízejí, ale při běžném prohlížení webu se tento protokol neaktivuje. Tento nenápadný doplněk stačí nainstalovat a on se pak už vždy postará o to, aby byl zabezpečený protokol HTTPS aktivován všude tam, kde je k dispozici. |

**Používání VPN** – „*virtuální privátní síť*“ nám umožňuje připojit se do sítě univerzity z domova a využívat tak všech služeb a výhod naší instituce, jako bychom byli přímo na univerzitě. Internetový provoz je při využití technologie VPN šifrován, takže nikdo nemůže zachytit, pozměnit nebo dokonce monitorovat naši aktivitu.

|  |
| --- |
| **Víte že...** VPN můžete využít například pro přístup k placeným elektronickým odborným zdrojům z domova? Využijte ji ale i pro mnoho dalších činností. Návody ke zprovoznění VPN na naší univerzitě najdete na <school-specific>*.* |

**Šifrování datových úložišť** – zatím jsme si využití šifrování ukazovali především v oblastech, kde informace někam putují. Šifrovat ale můžeme i ty informace, které někde ukládáme a nikam se neposílají – třeba soubory v našem počítači nebo v telefonu. I ty mohou být ohroženy, například když dojde k odcizení našeho zařízení. Nebo si upřímně odpovězte na otázku, kolikrát jste někde zapomněli svou USB paměť tak, že k ní a k datům na ní mohl mít přístup v podstatě kdokoliv...? Kdyby byla tato „*fleška*“ šifrována, bez klíče by se k nim žádný náhodný nálezce nedostal.

|  |
| --- |
| **Vyzkoušejte si...** šifrování externí USB paměti ve Windows. Nebudete k tomu potřebovat žádnou speciální aplikaci, šifrovací nástroj BitLocker je implementován přímo do operačního systému Windows. Připojte USB paměť, v průzkumníku Windows klikněte pravým tlačítkem na její ikonku a zvolte možnost Zapnout nástroj BitLocker. Dalším procesem už vás systém provede. Jen nezapomeňte heslo, které k zašifrování USB paměti použijete – uložte si ho třeba do správce hesel <odkaz slovník>. Také pozor: disk zašifrovaný nástrojem BitLocker rozšifrujete pouze na zařízeních s Windows. |

Tam, kde se pracuje s citlivými informacemi, se šifrují i pevné disky v počítači. Představte si, že útočník odcizí fyzicky váš notebook – nezná vaše heslo do systému Windows, ale to mu nezabrání dostat se k vašim datům uloženým v notebooku. Jak? Jednoduše počítač otevře a pevný disk z něj vyndá. Následně ho připojí ke svému počítači a k datům na vašem HDD se tak bez potíží dostane. Ovšem pouze za předpokladu, že váš pevný disk nebyl zašifrovaný – v takovém případě bude mít útočník smůlu.

Šifrování je silná technologie, ale může být i zneužita.
Pojďme se ještě zastavit u tématu zálohování a ransomware.

# Zálohuji, zálohuješ, zálohujeme

Propočty jsou to možná trochu divoké, ale uvádí se, že jen v USA každý týden selže na 140 000 pevných disků. Ve spěchu každodenní činnosti si mnohdy ani neuvědomíme, co by se stalo, kdyby zrovna náš disk odešel do věčných lovišť. Ve chvatu digitálních životů necháváme soubory na ploše v počítači nebo ve složce Dokumenty na lokálním zařízení, na telefonu nebo třeba tabletu. Tam naše data nejvíce ohrožují dvě hrozby: **nečekané selhání zařízení** (resp. pevného disku) a hrozba zvaná **ransomware**. Četli jste příběhy v prvním modulu? Tak to už jste o ransomware útocích slyšeli.

## Ransomware

Ransomware je záškodnický program, který si v nepozornosti stáhneme z podvrženého e-mailu nebo se k nám bez našeho vědomí nastěhuje při návštěvě napadeného webu. Ransomware pak zašifruje naše data, zablokuje nám přístup k zařízení a za zpětné rozšifrování dat žádá výkupné. Výkupné se většinou platí v anonymních digitálních měnách – a nebývá to málo peněz.

|  |
| --- |
| **Víte že...** průzkum agentury Sophos *State of Ransomware 2021* ukázal, že průměrná hodnota zaplaceného výkupného se pohybuje kolem 3,6 milionu korun, mediánová hodnota pak kolem 200.000 Kč? Jen 8 % napadených institucí ale dostane zpátky skutečně úplně všechna data, která byla zašifrována; 29 % pak ne víc než polovinu původních dat. Přesto mnoho z nich zaplatí: k datům se nemají jinak jak dostat, protože neřešili zálohování. A ransomware se samozřejmě týká i fyzických osob. |

Ransomware vás často také postaví do časové tísně: "*pokud nezaplatíte co nejrychleji, začnu mazat vaše soubory.*" Zákeřný ransomware Jigsaw a jeho následné varianty například po zašifrování vašich souborů každou hodinu několik smažou – čím déle otálíte s placením výkupného, tím více vašich souborů nezvratně mizí. Pokud nezaplatíte do 72 hodin, smaže se všechno. Desítky variant a klonů ransomwaru Jigsaw zákeřnou časovou strategii převzalo; dnes navíc ještě třeba vyhrožují tím, že vaše citlivá data a soubory zveřejní.

|  |
| --- |
| **Víte že...** někteří kyberzločinci mají zákaznické linky? Skutečnost, že třeba nevíte jak funguje Bitcoin a kde ho získat není pro útočníky žádný problém: některé ransomware mají odkaz na chat s živou podporou: pracovník "zákaznického" centra vás hezky uvítá, vše vám vysvětlí a celým procesem placení výkupného za svá data vás provede. Byznys je byznys a kyberkriminalita se v posledních letech výrazně profesionalizovala. Když ale zálohování věnujete pár chvil, ušetříte si čas, nervy i finance. |

|  |
| --- |
| Jak se tedy ransomware útoku bránit? * Nainstalujte si antivirus a udržujte ho aktualizovaný.
* Aktualizujte i všechny své programy, webové prohlížeče a operační systém.
* **Zálohujte svá důležitá data**.
 |

## Co zálohovat?

Prioritizujte! Ne všechny soubory jsou si rovny, některé jsou důležitější než jiné. Rozepsaná diplomka nebo draft odborného článku mají zcela jistě vyšší hodnotu než vtipné obrázky stažené z Facebooku. Až ransomware zaútočí, kvůli veselým GIFům s koťátky nejspíš nebudeme peněženku ani otevírat – kvůli bakalářce ve stavu téměř před odevzdáním už ale v zoufalství možná prasátko rádi rozbijeme. Není proto třeba zálohovat úplně všechno, ale hodí se rozsegmentovat si soubory: vyberte to nejdůležitější, nejzásadnější.

## Lokálně nebo v cloudu?

Zkopírovat si zálohu rozepsané diplomky z plochy na externí flash paměť není nejoptimálnější cesta – ale i to je lepší než vůbec nic. Jaké jiné možnosti ale máme?

**Záloha do cloudu.** Asi nejčastěji dnes využívanou metodou je tzv. záloha do cloudu. V cloudu máme data zálohovaná okamžitě a kdykoliv přístupná i z našich ostatních zařízení. Většinou vše jednou nastavíme a pak na zálohování můžeme zapomenout – vše se děje automaticky. Skutečnost, že jsou data "někde online v cloudu" sebou však nese jiná bezpečnostní rizika a je dobré se řídit radami ohledně pevného hesla a 2FA (viz modul 2). V rámci univerzity využíváme pro cloudové ukládání souborů platformu *<school-specific>*. Více informací a návody najdete na *<school-*specific>.

|  |
| --- |
| **Pozor!** Ani cloud není imunní proti ransomware útokům. Pokud mám na PC nastavené zálohování do cloudového úložiště a stanu se obětí ransomware útoku, zasáhne to i moje soubory v cloudu? Teoreticky ano. Pokud využíváte cloudové úložiště jako je Google Drive nebo OneDrive a máte na svém zařízení nainstalovaný program, který se automaticky stará o nahrávání vašich souborů do cloudu a o jejich aktualizaci, může se stát, že zákeřný ransomware soubory zašifruje a nic netušící aktualizační program nahradí soubory v cloudu zašifrovanými verzemi. Většina cloudových úložišť to ale vyřeší za vás: třeba OneDrive si sám všimne, že změny souborů vykazují známku ransomware útoku a provede nás procesem obnovy souborů. |

**Lokální záloha** může probíhat na externí média. Nikdo dnes už asi nezálohuje vypalováním na CD nebo DVD nosiče, ale takový externí pevný disk může být dobrá volba. I zde lze zálohování zautomatizovat: existují programy, které po připojení externího disku umí automaticky odeslat zálohy přednastavených souborů a složek na disk tak, abychom to nemuseli dělat ručně. Možná řešení konzultujte s IT podporou <school-specific>. Je však třeba myslet na to, že zálohy musíme dělat pravidelně, a že nemůžeme nechávat externí disk připojený k zařízení konstantně – až přijde ransomware, zašifruje i připojená externí média (včetně třeba takové USB paměti) a zálohy na externích nosičích mu tak mohou podlehnout taky.

|  |
| --- |
| **To nejdůležitější:*** Je dobré zálohovat důležité soubory, protože o ně můžeme lehko přijít.
* Kromě nečekaného selhání pevného disku nás může ohrozit i ransomware.
* Ransomware zašifruje naše data a za přístup k nim bude žádat výkupné.
* Když máme data někde zálohována, bolí nás tahle nepříjemná situace méně.
* Zálohovat se dá do cloudu (OneDrive atp.) nebo lokálně (externí pevný disk atp.).
 |

|  |
| --- |
| **Pozor!** **Co dělat, když se něco pokazí?** V případě, že došlo k bezpečnostnímu incidentu nebo máte podezření, že mohlo být narušeno vaše kyberbezpečí, obracejte se na <school-specific: doplňte kontaktní osobu nebo popište proces řešení kyberbezpečnostních incidentů>. |