ZÁKLADY POČÍTAČOVÉ BEZPEČNOSTI

Doc. Mgr. Kamil Kopecký, Ph.D.

**Podpora kompetencí vedoucích pedagogických pracovníků
při implementaci digitálních technologií do života školy/školského zařízení**

STUDIJNÍ TEXTY K DISTANČNÍMU VZDĚLÁVÁNÍ

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

Pedagogická
fakulta

Univerzita Palackého
v Olomouci

Tato publikace je výstupem projektu Kompetence leadera úspěšné školy,
reg. č. CZ.02.3.68/0.0/0.0/16_032/0008145

Jméno řešitele: Ing. Alena Opletalová, Ph.D.

Název díla: Základy počítačové bezpečnosti
Autor: Doc. Mgr. Kamil Kopecký, Ph.D. a řešitelský kolektiv projektu Centra celoživotního vzdělávání Pedagogické fakulty Univerzity Palackého v Olomouci.

URL autora: www.ccv.upol.cz
URL odkaz na původní dílo: www.klus.upol.cz

ZÁKLADY POČÍTAČOVÉ BEZPEČNOSTI

OBSAH

CÍLE DISTANČNÍHO TEXTU

- Seznámit s problematikou počítačové bezpečnosti se zaměřením na bezpečnost lokálních počítačových sítí (LAN) a zabezpečení operačních systémů desktopových počítačů.
- Seznámit se základy počítačové bezpečnosti; s metodami ochrany počítačové sítě a ochrany běžné desktopové stanice; s postupy při řešení incidentů a běžnými bezpečnostními standardy.

1 ZÁKLADY POČÍTAČOVÉ BEZPEČNOSTI

Internet je velmi užitečným nástrojem, který svým uživatelům nabízí nepřeberné množství možností, je to prostor pro komunikaci, vzdělávání a také zábavu, je také v současnosti primárním zdrojem informací všeho druhu. Bohužel je také prostředím, ve kterém může být náš počítač, tablet či mobilní telefon vystaven velkému množství hrozeb, proto je třeba zajistit bezpečnost jak jednotlivých zařízení, která internet využívají, tak i samotné počítačové sítě, která je k internetu připojena.

V našem textu se zaměříme na to:

1. Jak zabezpečit lokální síť a jak správně nastavit router.
2. Jakým způsobem zabezpečit samotná zařízení, která jsou do naší sítě připojena (tj. počítače, tablety, notebooky apod).

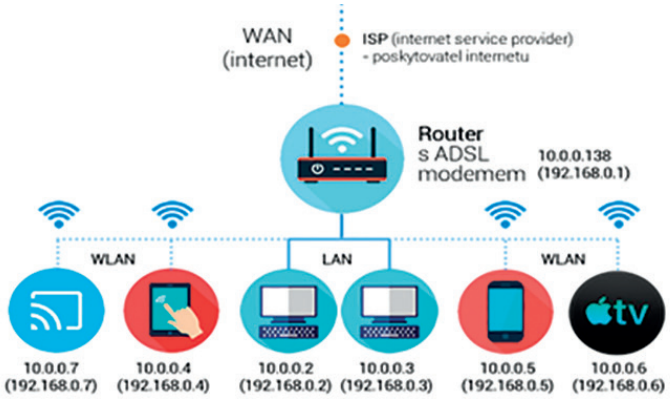
1.1 Zabezpečení lokální sítě

Domácí síť je složena z několika vzájemně propojených zařízení (počítačů, tiskáren apod.), která jsou připojena různými způsoby k tzv. routeru. Router je zařízení, které má celou řadu funkcí. Na prvním místě poskytuje domácnosti/škole přístup k internetové síti, je základním vstupním a výstupním bodem do/ze světa internetu. Router propojuje dvě sítě – tzv. WAN síť (wide area network, rozlehlá síť, která pokrývá rozlehlé geografické území, např. síť poskytovatele internetového připojení připojená k internetu) a LAN síť (lokální, místní síť, tj. naše domácí síť). Mezi těmito dvěma sítěmi pak router usměrňuje (routuje) tok informací (tzv. datový tok).

Nejjednodušším způsobem, jak lze router připojit k internetu, je připojení pomocí běžné digitální telefonní linky. K tomu potřebujeme router, který je zároveň zkombinován s DSL/ADSL/VDSL modemem. Ten umí využít pro připojení k internetu digitální telefonní linku (jejíž kapacita trvale roste) a je tedy využíván především v domácnostech či menších školách.

Router je velmi důležité síťové zařízení a z hlediska bezpečnosti domácnosti, školy či jiné instituce je velmi důležité jeho zabezpečení. Přes nezabezpečený router může útočník proniknout do naší domácí sítě, napadat naše počítače, získat přístup k IP kameře či dalším zařízením, které jsou do domácí sítě připojeny, získávat potenciálně zneužitelná data atd.

Router však není pouze přístupový bod do světa internetu, umožňuje toho podstatně více – např. vytvořit lokální síť (LAN), ale také lokální bezdrátovou sít (lokální „wifinu“, tzv. WLAN), poskytuje nám přístup k online televizi (IPTV), router nám umožňuje připojit do sítě různé druhy datových úložišť (NAS), která nám umožňují např. streamovat video a hudbu, ale také zálohovat, synchronizovat a sdílet naše privátní soubory apod.



Obrázek 1: Mapa jednoduché sítě připojené k internetu (zdroj: Kamil Kopecký)

1.1.1 Jak zabezpečit router?

Každému routeru je po spuštění a připojení do počítačové sítě přidělena unikátní adresa – tzv. IP adresa, která je složena ze 4 čísel oddělených tečkou (tzv. IP4). Router má nejčastěji IP adresu 10.0.0.138 nebo 192.168.0.1 (výrobce vždy výchozí adresu routeru uvádí v manuálu k obsluze). Pokud se k routeru připojí další zařízení (počítač, mobilní telefon, domácí asistent, externí datové úložiště apod.), automaticky od routeru obdrží vlastní IP adresu (pomocí tzv. DHCP, dynamic host configuration protocol), pod kterou je v rámci lokální sítě identifikovatelné. Router tak neustále sleduje veškerá zařízení, která jsou k němu připojena.

Pokud chceme mít router dostatečně zabezpečen, je nutné zajistit následující:

1. Změnit výchozí heslo k administraci routeru

Každý router má nastaveno výchozí heslo pro vstup do jeho administrativní části. Zpravidla jde o spojení přihlašovacího jména a hesla admin/admin nebo root/root apod. Při prvním přihlášení k routeru doporučujeme výchozí heslo změnit. K routeru se přihlásíme zadáním IP adresy routeru do běžného webového prohlížeče (10.0.0.138 nebo 192.168.0.1) – podobně jako když otevíráme běžnou internetovou stránku.

2. Pravidelně aktualizovat operační systém routeru, tzv. firmware

Stejně jako u operačního systému běžného desktopového počítače je velmi důležité udržovat software routeru stále aktuální. Proto je důležité pravidelně software routeru – tzv. firmware – aktualizovat. Většina routerů má tuto funkci dostupnou v rámci administrativního prostředí.

3. Veškeré bezdrátové sítě vytvořené routerem opatřit heslem

Jak již bylo řečeno, většina routerů umožňuje vytvářet vlastní lokální bezdrátové sítě, tzv. WLAN. Bezdrátovou síť nastavíme přímo v administrativním prostředí routeru – na jedné straně vybereme vhodný název sítě (tzv. SSID) a poté volíme, jak bude přístup k síti zabezpečen (např. heslem). Beztrátovou síť vždy opatřeme vstupním heslem pod zabezpečením WPA2-PSK. Starší typy zabezpečení (WEP apod.) jsou považovány za zastaralé a prolomené.

Moderní routery zpravidla umožňují uživatelům vytvářet bezdrátové domácí sítě operující ve dvou frekvenčních pásmech – 2,4 GHz a 5 GHz, u obou je nutné nastavit zabezpečení na WPA2-PSK.

4. Filtrovat připojení nežádoucích zařízení do naší sítě

Jak jsme si již vysvětlili v předchozí části, router sleduje, která zařízení jsou k němu připojena. Zařízení router identifikuje podle IP adresy, kterou mu router přidělil, ale také podle tzv. MAC adresy (ta je na IP adrese nezávislá). MAC adresa je tzv. fyzická adresa, která je přiřazována síťové kartě daného zařízení, třeba notebooku, tabletu či běžného PC. Skládá se

z šesti dvojciferných hexadecimálních čísel oddělených pomlčkami či dvojtečkami. Přestože byla MAC adresa původně navržena jako neměnná, u moderních síťových karet je možné ji změnit (virtuálně).

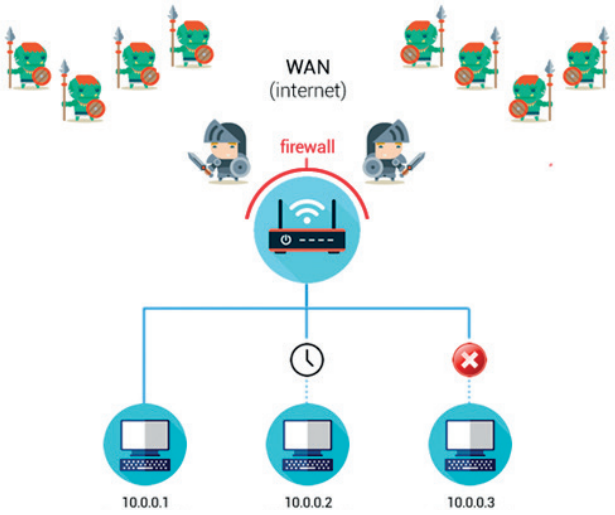
5. Filtrovat nežádoucí obsah prostřednictvím systémů rodičovské kontroly

Moderní routery umožňují nastavit, jaký obsah bude možné (či nemožné) z konkrétního počítače (či celé LAN) zobrazovat. Router totiž umožňuje filtrovat přístup k obsahu právě z konkrétní MAC adresy – nezávisle na IP adrese, kterou dostal daný počítač přidělenu. To platí pro veškerá zařízení – mobilní telefony či tablety, které využívají router pro přístup k internetové síti. Některé routery také umožňují regulovat čas, ve kterém mohou daná zařízení přistupovat na internet.

6. Mít aktivní firewall routeru

Firewall si můžeme jednoduše představit jako „stráž vstupu do hradu", která rozhoduje o tom, koho/co pustí dovnitř a co ven. Úkolem firewallu je bránit místní síť před různými druhy útoků, firewall totiž filtruje příchozí a odchozí data.

Firewall umožňuje filtrovat obsah, ke kterému se na internetu dostaneme, a to pomocí zákazu konkrétních internetových adres či jejich částí (URL). Pomocí firewallu tak lze např. blokovat všechny stránky, které obsahují slovo *porn*, *facebook* apod. Firewall také umí filtrovat konkrétní síťové služby (třeba stahování a odesílání pošty, otevírání www stránek apod.) – a to pomocí blokování konkrétních portů, na kterých služby běží (port je vlastně číslo od 0 do 65535, které označuje konkrétní službu, kterou počítač používá, např. port 80 je port pro http služby, tj. otevírání webových stránek). Pomocí zákazu portů lze také např. blokovat používání konkrétních komunikačních nástrojů, třeba messengerů (Skype).



Obrázek 2: Router v lokální síti (zdroj: Kamil Kopecký)

1.2 Zabezpečení koncového zařízení

Pro zabezpečení koncového zařízení – zpravidla počítače – je nutné dodržet několik jednoduchých zásad:

1. Používejme legální software

Základním pravidlem, které je třeba pro zajištění bezpečnosti počítačové stanice dodržet, je používání legálního software – především legálního operačního systému. Legální operační systém s sebou nese řadu výhod – je pravidelně aktualizován a „záplatován", čímž se minimalizuje riziko útoku prostřednictvím existujících chyb a děr; legální systém je stabilní (o což se také starají pravidelné aktualizace); lze jej snadno upgradovat např. na vyšší a pokročilejší verze a samozřejmě také nehrozí riziko finančního postihu za používání nelegálního software, kterému jsou uživatelé nelegálních „pirátských" kopií vystaveni. Stejné pravidlo platí i pro aplikace, které do počítačového systému instalujeme.

2. Operační systém a nainstalované aplikace udržujme vždy aktuální

Základem dobře zabezpečeného počítače je aktuální operační systém a aktualizované aplikace. Aktualizace především opravují chyby, prostřednictvím kterých by se do našeho počítače mohli dostat jak živí útočníci, tak různé druhy počítačových virů.

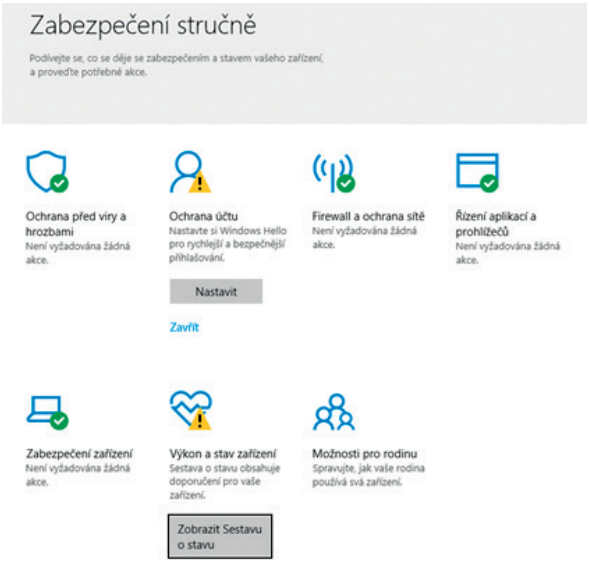
3. Pravidelně aktualizujme všechny aplikace, které máme na počítači nainstalovány

Stejně tak je důležité pravidelně aktualizovat všechny aplikace, které máme v počítači nainstalovány a které by se mohly stát nástrojem útoku. Důsledně aktualizujme především internetové prohlížeče, které používáme pro přístup k internetovým službám nejčastěji – právě pomocí internetových prohlížečů probíhají útoky velmi často.

4. Používejme firewall

Stejně jako routery, tak i operační systémy mívají integrován firewall, který se chová podobně jako firewall v routeru. Firewall v operačním systému umožňuje nastavit pravidla pro výměnu dat s internetem podstatně detailněji – na úrovni konkrétních aplikací či jejich portů. Snadno tak můžeme zakázat či povolit komunikaci konkrétních aplikací s internetem.

Novější operační systémy Windows 10 obsahují nástroj Windows Defender, který je kombinací antivirového programu a firewallu a který obsahuje další bezpečnostní části (např. řízení uživatelských účtů, řízení aplikací, sledování výkonu apod.). Poskytují tak uživatelům minimální bezpečnostní standard bez nutnost instalovat další přídavné bezpečnostní aplikace.



Obrázek 3: Bezpečnostní nástroje Windows 10 (Zdroj: MS Windows 10)

5. Používejme antivirové programy

Přestože novější operační systémy obsahují integrovanou antivirovou ochranu, je přesto velmi dobré vylepšit si ochranu svého počítače kvalitním antivirovým programem. Antivirové programy umožňují v reálném čase otestovat jakýkoli soubor, který na našem počítači otevřeme, chránit internetové prohlížeče, detektovat hrozby skryté v komprimovaných souborech, odhalit tzv. phishing (technika útoku zaměřená na získání osobních a citlivých údajů – např. pro vstup do internetového bankovnictví), apod.

Nelze říci, který antivirový program je v současnosti nejlepší, řídit se můžeme např. různými druhy recenzí a statistik, ve kterých pravidelně dominuje přibližně 5 antivirových produktů.

Tabulka 1: Nejlepší antivirové programy 2019

	Antivirový program	Pořadí v testu Nejlepší antivir roku 2019	Pořadí v testu Nejlepší antivir roku 2019	Pořadí v testu Nejlepší antivir roku 2019
	Eset Family Security	1	2	6
	Kaspersky Internet Security	2		1
	AVG Internet Security	3	4	4
	Avast Internet Security	4	1	3
	Norton Security Deluxe	5	3	5
	McAfee AntiVirus Plus		5	
	BitDefender Internet Security			2
		Testado.cz	5nej.cz	Arecenze.cz

Základním úkolem antivirových programů je především odhalit nebezpečné programy – počítačový viry (malware). Těch existuje celá řada.

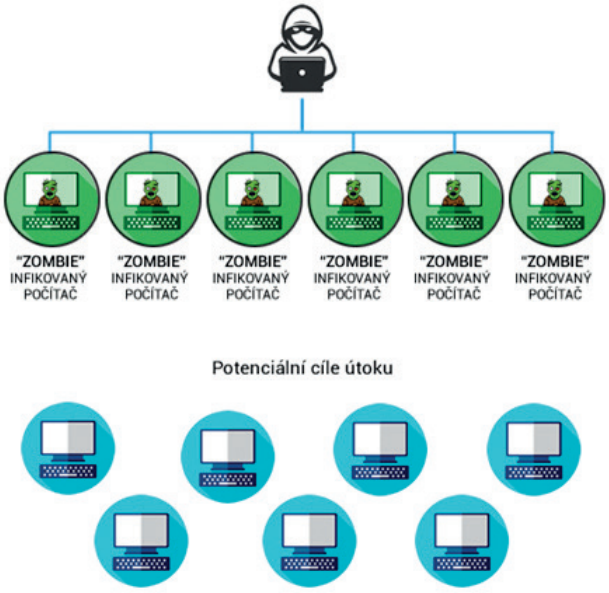
Tabulka 2: Základní druhy nebezpečného obsahu

Druh nebezpečného programu	Co dělá
Počítačový červ	Nepotřebuje k šíření hostitelský program. Jakmile napadne počítač, začne své kopie bez vědomí uživatele posílat na další počítače a „prolézá“ tak internetem.
Trojský kůň / backdoor	Na první pohled vypadá jako užitečný program, nicméně umožňuje svému tvůrci otevřít do počítače „zadní vrátka“ a proniknout do něj.
Spyware	Program, který z počítače tajně odesílá data – třeba vaše soubory.
Adware	Program, který na počítači bez souhlasu uživatele zobrazuje reklamy (vyskakovací okna v prohlížeči).

Stalkerware	Program, který umožňuje nepozorovaně vniknout do soukromého života cizího člověka a získávat o něm informace, fotografie, přístup k sociálním sítím apod. Často se využívají v rámci „partnerské špionáže“.
Ransomware	Zablokuje vám počítač a nutí zaplatit částku za odblokování. Vyhrožuje vám např. tím, že jste spáchali trestný čin a musíte uhradit pokutu. Do této skupiny řadíme tzv. policejní viry.
Rootkit	Program, který v operačním systému skrývá svou přítomnost a je úzce propojen s operačním systémem a který může negativně ovlivnit jeho chod, umožňuje hackerům vstupovat do operačního systému, apod. Běžný antivirový program jej detekuje velmi obtížně.

Dalšími nepříjemnými programy jsou tzv. **botneti/botnety** – programy, které v pozadí operačního systému provádějí automaticky různé nežádoucí činnosti, jako je třeba rozesílání spamů či DDoS útoky (denial of service, útoky postavené na přetížení konkrétního počítačového serveru, který pak přestane fungovat a uživatelé se k němu nepřipojí). O výskytu botů ve svém počítači často uživatelé neví, počítač je pouze pomalejší než obvykle, pomalejší je také internetové připojení, které je využíváno k šíření virové nákazy.

Jak již složenina bot-net napovídá, botnety tvoří celé sítě infikovaných počítačů, které lze ovládat z jednoho centra. Napadené počítače se pak označují jako **zombies** (zombie computers). Botnety umožňují samozřejmě šířit adware, spyware, ransomware, spam apod.



Obrázek 4: Struktura botnetu (Zdroj: Kamil Kopecký)

6. Uživatelské účty mějme vždy zabezpečeny bezpečným heslem

Veškeré uživatelské účty, které používáme, je nutné mít zabezpečeny kvalitním a silným heslem. Nároky na kvalitu hesla se postupem času zvyšují; nyní by např. dle firmy Avast (Empey, 2019) mělo **optimální heslo obsahovat 9–12 znaků (kombinace velkých a malých písmen, číslic, speciálních znaků)**, nemělo by být obsaženo v běžných slovnících a nemělo by být univerzální (stejné heslo pro přístup ke kritickým účtům), apod. Pokud zkombinujeme více slov za sebe (AutobusZebraKladivoChlor), heslo slovníkovému útoku odolá.

Silné heslo si můžeme nechat také vygenerovat pomocí online nástrojů, jako je např. *https://www.avast.com/random-password-generator*. Problémem je však zapamatovatelnost hesla – vygenerované heslo si velmi obtížně zapamatujeme. Výhodou češtiny je její diakritika, silné heslo lze proto vytvářet tak, že diakritické značky ve slovech nahradíme číslicemi na příslušných klávesách – tedy např. „červenéjablíčko" = 4erven0jabl94ko. Tímto způsobem lze vytvořit silná a velmi bezpečná hesla.

Pro účty, které se nacházejí v online prostředí, doporučujeme používat tzv. **dvoufaktorové ověření**, které se dříve využívalo především v bankovním sektoru. V praxi to znamená, že kromě běžného hesla využijeme pro přístup k online účtu mobilní telefon – po zadání hesla musíme přihlášení navíc potvrdit speciálním kódem, který nám systém zašle SMS zprávou do našeho mobilního telefonu. Ačkoli se nám tato procedura dvojího zadávání hesel může zdát zbytečná a únavná, zásadně zvyšuje bezpečnost našeho online účtu. Možností je také přihlašovat se s použitím speciálního hardwarového klíče, který připojíme do USB portu – tento způsob přihlašování však drtivá většina běžných uživatelů nepoužívá.

Čas od času dojde k úniku přihlašovacích údajů do online prostředí (ať už prostřednictvím hackerského útoku či jinak), a proto je nutné heslo pravidelně změnit. V roce 2013 např. unikly do online prostředí přihlašovací údaje 153 milionů uživatelských účtů firmy Adobe, v roce 2012 údaje 10 milionů uživatelů Dropboxu, v roce 2016 164 milionů přihlašovacích údajů LinkedInu, apod. Na webových stránkách Have I Been Pwned? *https://haveibeenpwned.com/* si můžete otestovat, zda vaše přihlašovací údaje neunikly do online prostředí.

Zkoumáním kvality hesel se zabývá např. britské Národní centrum pro kybernetickou bezpečnosti (NCSC). Odborníci z NCSC analyzovali právě databázi Have I Been Pwned? a zjistili, že nejčastějším heslem byla kombinace znaků 123456 (23,2 milionů účtů), 123456789 (7,7 milionů účtů), qwerty (3,8 milionů účtů), password (3,6 milionů účtů) a 111111 (3,1 milionu účtů). Seznam 100 000 nejčastějších hesel je pak k dispozici zde: https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordTop100k.txt.

Pokud používáte prohlížeč Chrome, můžete využít rozšíření *Password Checkup* (v češtině Kontrola hesel), které vyvinula firma Google. Toto rozšíření automaticky varuje uživatele, pokud se hlásí ke službě uživatelským jménem nebo heslem, které se objevilo v některém z úniků přihlašovacích údajů, která má Google k dispozici. (Caletka, 2019)

Velký problém představují především tzv. **univerzální hesla** – uživatelé používají pro přístup k různým službám stejné heslo. Pokud pak unikne heslo z jedné služby, v ohrožení jsou okamžitě i účty na ostatních službách. Pro každou službu proto doporučujeme používat jiné heslo.

Při nastavení účtu **nezapomeňme nastavit možnosti obnovení hesla** pro situace, kdy heslo zapomeneme. Některé služby umožňují heslo (či kód k resetování hesla) zaslat na e-mail, případně na mobilní telefon (SMS s jednorázovým kódem pro resetování hesla). Některé účty také požadují vyplnit kontrolní otázky – volme vždy takové otázky, na které známe odpověď pouze my, a ne jiné osoby (ITSEC-NN, 2018).

Základní pravidla spojená s používáním hesel:

1. Vytvořte si silné heslo.
2. Pro každou službu používejte jiné heslo.
3. Udržujte si o svých heslech přehled.
4. Nastavte si možnosti obnovení hesla.
5. Používejte dvoufázové ověřování.
6. Heslo si nikdy nezapisujme např. na spodní část klávesnice či na lísteček nalepený na monitor počítače. To platí také např. pro platební kartu – pin k platební kartě nezapisujme ani na kartu, ani na lísteček, který pak vložíme do peněženky do blízkosti platební karty.

7. Nezapomínejme na zabezpečení tabletu či chytrého telefonu

Stejná bezpečnostní opatření, která provádíme na běžném počítači (desktop, notebook), bychom měli provést také na tabletu či chytrém mobilním telefonu (smartphony). I pro tato zařízení existují antivirové programy a další bezpečnostní pomůcky. Ve spojení s mobilním telefonem však hrozí další vážné riziko: možnost infikování mobilního telefonu neověřenou aplikací (staženou z neověřeného zdroje, ale také např. z Google Play), která převezme kontrolu např. nad SMS zprávami.

Jak jsme si vysvětlili v předcházející části textu, u dvojfázového (dvoufaktorového) ověřování nám po zadání našich přihlašovacích údajů na mobilní telefon dorazí bezpečnostní kód, který nám umožní vstoupit do našeho účtu a např. provést finanční transakci – třeba platební příkaz. V případě infikovaného mobilního telefonu však SMS zprávu zachytí právě mobilní aplikace, která kód poskytne útočníkovi – ten pak může vstoupit do našeho účtu a provádět finanční transakce.

Příkladem takové aplikace byl např. QRecorder, který se tvářil jako pomůcka umožňující automatické nahrávání telefonních hovorů. Ve skutečnosti však pachatelé prostřednictvím této aplikace „odposlouchávali" důvěrné údaje, mimo jiné např. přihlašovací údaje k internetovému bankovnictví. Pachatelé si pak nechávali přeposílat autorizační SMS zprávy a získávali přístup k bankovním účtům. Na rizikovou aplikaci upozornila např. Česká spořitelna (ČSAS, 2018) a další bankovní instituce.

QRecorder však nebyl jedinou aplikací, která byla zaměřena na útok na mobilní telefon. Podle údajů antivirové společnosti ESET (Loucký, 2018) bylo v oficiálním obchodu s aplikacemi pro operační systém Android Google Play minimálně 6 dalších falešných bankovních aplikací, které okrádají uživatele o údaje o platebních kartách a přihlašovací údaje k internetovému bankovnictví. Na rozdíl od předešlé ztrojanizované aplikace QRecorder ale necílí primárně na české uživatele. I celkový objem instalací je podstatně nižší. Bezpečnostní společnost ESET objevila aplikace, které se vydávají za legitimní nástroje pro přístup k účtům bank z Nového Zélandu, Austrálie, Spojeného království, Švýcarska, Polska a rakouské směnárny kryptoměn Bitpanda. (Loucký, 2018)

Falešné aplikace byly do Google Play nahrány v červnu 2018 a do doby, než je společnost Google odstranila, byly více než tisíckrát staženy a nainstalovány. Aplikace byly do oficiálního obchodu nahrány pod různými jmény vývojářů a každá z nich vypadala jinak, nicméně podobnost jejich kódu naznačuje, že jsou dílem jednoho útočníka.

U mobilních zařízení je třeba dodržet následující kroky (převzato, upraveno a rozšířeno z doporučení České spořitelny):

1. Nainstalujte si antivir a pravidelně jej aktualizujte.
2. Provádějte pravidelnou aktualizaci softwaru vašeho chytrého telefonu.
3. Neprovádějte žádný zásah do operačního systému (jailbrake, root).
4. Před stahováním aplikací si pročtěte recenze – pokud uživatelé nemají kladnou zkušenost, raději se instalování aplikace vyhněte.
5. Pozorně čtěte informace při instalování různých aplikací – především u aplikací, které vyžadují příliš mnoho povolení k přístupu.
6. Většina malware si žádá, aby se stal administrátorem vašeho zařízení – takové povolení nedávejte a aplikaci neinstalujte.
7. Pokud se obáváte, že jste si nainstalovali podvodnou aplikaci, okamžitě ji odinstalujte, změňte PIN k platební kartě, přístupové údaje k internetovému bankovnictví a zároveň prověřte, zda na účtu neproběhla nějaká podezřelá transakce. Pokud ano, okamžitě informujte svou banku.

8. Pozor na webové kamery

Speciální pozornost doporučujeme věnovat právě webovým kamerám, kterými je vybavena drtivá většina mobilních zařízení. Kamery připojené k internetu jsou také běžnou součástí lokálních sítí, a to jak v domácnostech, tak i firmách a státních institucích včetně škol. Pro útočníky pak kamery představují jeden ze vstupních bodů do počítačových sítí. Jak potvrzuje firma Avast (Avast, 2019), počet nahlášených útoků na webové kamery roste.

Řada celebrit či osob, které zastávají významné funkce, si webkamery na noteboocích či tabletech přelepují. K nim patří např. James Comey, ředitel americké FBI, nebo Mark Zuckerberg, ředitel Facebooku. Důvodů, proč by někdo chtěl ovládnout naši webovou kameru, je celá řada – především jde o to získat co nejvíce citlivých informací, které lze zneužít např. k vydírání či záměrnému poškozování konkrétních osob.

Obrázek 5: Mark Zuckerberg má přelepenou webkameru (zdroj: Facebook.com, profil Marka Zuckerberga)

Aby se hackeři dostali k naší kameře např. na notebooku, musí nějakým způsobem napadnout operační systém našeho počítače. Napadení pak probíhá zpravidla prostřednictvím e-mailu, který obsahuje infikovanou přílohu. Ta do našeho počítače nainstaluje program pro vzdálený přístup k počítači (RAT – Remote Administration Tools). Ten pak umožňuje na dálku kameru ovládat – včetně možnosti vypnout signalizační LED diodu, která ukazuje aktivitu webkamery. (PC World, 2017)

Zkušenosti s útoky na webové kamery mají např. tisíce uživatelů erotických stránek v Austrálii, kteří se stali kvůli intimním záběrům pořízeným z napadených webkamer terčem vydírání. (Potůček, 2016) Hackeři ze zámoří využili pro útoky škodlivý program, jehož prostřednictvím mohli ovládat integrované webkamery na počítači nebo notebooku. Poté nahráli intimní záběry majitelů napadených zařízení a poslali jim e-mail s výhrůžkou, že pokud nezaplatí 10 tisíc dolarů, zašlou nahrávku jejich kolegům v práci nebo ji vyvěsí na Facebook. Podle australského serveru ABC čelily podobnému vyhrožování statisíce Australanů – útoky přicházely ze zahraničí a jejich původci jsou těžko dohledatelní.

Vlnu vydírání postavenou na intimních materiálech (tzv. sextortion), které fiktivní pachatelé získali právě z webových kamer, zažila také Česká republika. (Kopecký, 2018) Přestože v drtivé většině případů nedošlo k úniku citlivých údajů z webkamer ani počítačů obětí, už pouhý strach z toho, že by materiály skutečně mohli pachatelé mít, donutilo řadu uživatelů k zaplacení „výpalného". Varování zveřejnila také *Policie ČR*, která důsledně upozornila na to, aby uživatelé, kteří podezřelé emaily tohoto typu obdrželi, tyto e-maily ignorovali, nereagovali na ně, smazali je, označili za spam a v žádném případě nic neplatili.

2 SPECIFIKA POČÍTAČOVÉ BEZPEČNOSTI V PROSTŘEDÍ ŠKOLY

V předcházejícím textu jsme se zaměřili na základní bezpečnostní zásady spojené s počítačovými sítěmi i samotnými koncovými zařízeními. Ve školním prostředí je však třeba tyto zásady rozšířit o další doporučení. Jedním z nich je např. **regulace obsahu, ke kterému se žáci při používání běžných vyhledávacích služeb dostanou**.

Nejčastějším nástrojem, který děti i dospělí pro vyhledávání informací v online prostředí používají, je vyhledávač Google. Ten umožňuje ve standardním nastavení vyhledat v online prostředí jakékoli informace (s výjimkou vyloženě zakázaného obsahu), např. pornografii či extrémní obsah. Pokud mají žáci vyhledávač Google ve školní síti používat, je třeba prohlížeč nastavit do režimu tzv. *bezpečného vyhledávání*. Tento režim potom dětem odfiltruje obsah, který pro děti není vhodný (např. pornografii). Režim bezpečného vyhledávání by měl být nastaven nejenom na všech počítačích, které využívají žáci, ale také na počítačích učitelských, řídících. Podobně lze nastavit např. také server YouTube.

Další možností, jak regulovat přístup dětí k online obsahu, je využití **firewallového filtru** (na routeru), případně **systému rodičovské kontroly** (v rámci operačního systému). Zde lze nastavit, ke kterým službám bude mít žák přístup a ke kterým ne. Možnost nabízejí také různá externí řešení, jako je služba **OpenDNS**, která také umožňuje filtrovat závadný a nevhodný obsah.

Velmi důležité je také **zabezpečit USB vstupy počítačů a dalších zařízení**, ke kterým mají žáci ve škole přístup. Někteří z žáků totiž přinášejí z domova do školy různé druhy softwaru právě na USB klíčenkách a pomocí USB portů počítačů pak spouštějí nežádoucí aplikace, pomocí kterých pak používají školní internet, případně pronikají do počítačů připojených do školní sítě. Příkladem takových aplikací mohou být různé druhy „portable" verzí prohlížečů (tj. přenosných verzí prohlížečů, které není třeba instalovat), skrze něž se dostanou k obsahu, který nainstalovaný prohlížeč jinak blokuje.

Velkým (nejenom bezpečnostním) problémem současnosti je využívání mobilních telefonů žáků v prostředí školy. Podle výzkumu *České děti v kybersvětě* (2019) totiž **více než polovina českých žáků (59 %) potvrdila,** že mají ve svém mobilu trvalý přístup k internetu a jsou v zásadě na školní či jiné WiFi nezávislí. To znamená, že přestože má škola zabezpečenou počítačovou síť a nastaveny případné filtrace nežádoucího obsahu/služeb, dítě se přesto dostane k online obsahu nezávisle na provedených opatřeních. (Kopecký, 2019) Za to, jakým způsobem má dítě zabezpečen mobilní telefon, by však měli nést odpovědnost především rodiče dítěte, nikoli škola.

Jednotný není ani způsob, jak české školy využívání mobilních telefonů ve výuce regulují – část škol má používání mobilních telefonů zakázáno ve vyučovacích hodinách a o přestávkách, část pouze ve vyučovacích hodinách – a o přestávkách je mobilní telefon povolen. Diskuse, jak s mobilními telefony v prostředí školy nakládat v budoucnu, neustále probíhá nejen v České republice, ale také v dalších zemích Evropy. V ČR pak tato diskuse rozdělila školy na dva přibližně stejné tábory obhájců a odpůrců využívání mobilních telefonů o přestávce.

Poznámka: Autor tohoto textu se kloní – na rozdíl od České školní inspekce – k regulaci používání mobilního telefonu jak o přestávkách, tak v*e vyučovacích* hodinách. Své argumenty shrnuje na: *www.e-bezpeci.cz*

SHRNUTÍ

- Internet je velmi užitečným nástrojem, bohužel je také prostředkem, ve kterém může být náš počítač, tablet či mobilní telefon vystaven množství hrozeb. Je proto potřeba zajistit bezpečnost jednotlivých zařízení, která internet využívají, i samotné počítačové sítě, jež je k internetu připojena.
- Důležitým síťovým zařízením je pro domácnosti, školy a jiné instituce router. Umožňuje také vytvořit např. lokální síť (LAN) aj. Pro jeho zabezpečení je nutné: změnit výchozí heslo k jeho administraci; pravidelně aktualizovat jeho operační systém (firmware); veškeré bezdrátové sítě vytvořené routerem opatřit heslem; filtrovat připojení nežádoucích zařízení do naší sítě; filtrovat nežádoucí obsah prostřednictvím systémů rodičovské kontroly; mít aktivní firewall routeru.
- Pro zabezpečení koncového zařízení (zpravidla počítače) je nutné dodržovat tyto zásady: používat legální software; udržovat aktuální operační systém a nainstalované aplikace; pravidelně aktualizovat nainstalované aplikace; používat firewall; používat antivirové programy (výčet nejlepších je uveden v textu); uživatelské účty mít vždy zabezpečeny bezpečným heslem (pravidla pro vytvoření jsou uvedena v textu).
- Stejná bezpečnostní opatření je třeba provádět i na tabletech či chytrých telefonech.
- Speciální pozornost je třeba věnovat webovým kamerám – pro útočníky představují jednu ze vstupních bran do počítačových sítí.
- Ve školním prostředí je nutno všechny výše uvedené zásady rozšířit o další doporučení: např. regulace obsahu, ke kterému se žáci při používání běžných vyhledávacích služeb dostanou; zabezpečení USB vstupů aj. zařízení, k nimž mají žáci přístup; učinit zodpovědná rozhodnutí, jak přistupovat k používání mobilních telefonů (většina žáků má na svých telefonech trvalý přístup k internetu) ve škole.
- Bezpečnostních hrozeb a způsobů je však podstatně více, než bylo uvedeno v textu (jejich detailní popis by zabral desítky hodin). Proto doporučujeme sledovat a odebírat následující internetové stránky: *www.e-bezpeci.cz*, *www.chip.cz, www.dvojklik.cz, www.avast.com, www.hoax.cz* apod. Zde naleznete aktuální novinky ze světa online bezpečnosti a způsoby, jak se v online světě účinným způsobem bránit.

Kontrolní otázky a úkoly

1. *Vyjmenujte alespoň 5 základních doporučení pro zabezpečení routeru.*
2. *Vyjmenujte alespoň 5 základních způsobů pro zabezpečení osobního počítače.*
3. *Uveďte, jaké vlastnosti by mělo splňovat bezpečné heslo.*
4. *Popište, co je dvojúrovňové zabezpečení.*
5. *Uveďte alespoň 3 příklady tzv. malware.*

POUŽITÁ LITERATURA

EMPEY, Ch., 2019. Jak si nastavit silné heslo. In: *Avast Blog* [online]. Dostupné z: https://blog.avast.com/cs/jak-si-nastavit-silne-heslo

Eset, 2019. Prevence. *Přes 23 milionů kompromitovaných účtu používalo heslo "123456"* [online]. Eset. Dostupné z: https://www.eset.com/cz/blog/prevence/pres-23-milionu-kompromitovanych-uctu-pouzivalo-heslo-123456/

CALETKA, O., 2019. Rozšíření pro Chrome odhalí kompromitované účty. In: *Root.cz* [online]. Dostupné z: https://www.root.cz/zpravicky/rozsireni-pro-chrome-odhali-kompromitovane-ucty/

NETWORK NEWS, 2018. *Pouze 13 %* Čechů používá opravdu silná *hesla* [online]. ITSEC Network News. Dostupné z: https://www.itsec-nn.com/pouze-13-cechu-pouziva-opravdu-silna-hesla/

KOPECKÝ, K., 2019. Jak zabezpečit domácí počítačovou síť. *E-Bezpečí* [online]. 4(2), 44–48. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=1651

Česká spořitelna, 2018. Zprávy z banky. *Upozorňujeme na novou podobu počítačového viru* [online]. Česká spořitelna. Dostupné z: https://www.csas.cz/cs/zpravy-z-banky/2018/09/25/ upozorneni-na-novou-podobu-pocitacoveho-viru

LOUCKÝ, M., 2018. Falešné bankovní aplikace opět řádí v Google Play. In: *Chip* [online]. Dostupné z: https://www.chip.cz/novinky/falesne-bankovni-aplikace-opet-ridi-v-google-play/

PALYZA, J., 2019. Google nyní skenuje všechna vaše hesla: rozšíření pro Chrome chrání před úniky. In: *Chip* [online]. Dostupné z: https://www.chip.cz/novinky/google-nyni-skenuje-vsechna-vase-hesla-rozsireni-pro-chrome-chrani-pred-uniky/

EMPEY, Ch., 2019. 5 tipů na ochranu webové kamery před hackery. In: *Avast Blog* [online]. Dostupné z: https://blog.avast.com/cs/5-tip%C5%AF-na-ochranu-webove-kamery-pred-hackery

PC World, 2017. *Víte, proč byste si měli zakrývat webkameru na svém notebooku?* [online]. PC World. Dostupné z: https://pcworld.cz/hardware/vite-proc-byste-si-meli-zakryvat-webkameru-na-svem-notebooku-49414

POTŮČEK, J., 2016. Tisíce Australanů čelí vydírání kvůli intimním záběrům přes webkameru. In: *Eset – Dvojklik* [online]. Dostupné z: https://www.dvojklik.cz/tisice-australanu-celi-vydirani-kvuli-intimnim-zaberum-pres-webkameru/

KOPECKÝ, K., 2018. E-maily o tom, že pachatelé pomocí viru RAT získali vaše intimní materiály, jsou podvodné, jde o scam. *E-Bezpečí* [online]. 3(2), 45–47. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=1358

KOPECKÝ, K., 2019. Mobilní telefon ve škole – co dělají děti s mobilním telefonem o školních přestávkách?. *E-Bezpečí* [online]. 4(2), 38–43. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=1642

KOPECKÝ, K., 2018. Komentář: Zakázat mobilní telefon o přestávkách? *E-Bezpečí* [online]. 3(2), 1–4. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view= article&id=1316

KOPECKÝ, K. a SZOTKOWSKI, R., 2019. Komentář: O mobilních telefonech podruhé aneb Nemíchejme dohromady jablka, hrušky, švestky, broskve a mandarinky. *E-Bezpečí* [online]. 4(1), 26–33. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view =article&id=1438

POZNÁMKY

POZNÁMKY

PdF UP v Olomouci, Žižkovo nám. 5, 771 40 Olomouc

CENTRUM
CELOŽIVOTNÍHO
VZDĚLÁVÁNÍ

Centrum celoživotního vzdělávání

www.ccv.upol.cz