E-Bezpečí 2019, 4(2): Page 51-63. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1653

JAK ZABEZPEČIT POČÍTAČ

Kamil KOPECKÝ

V našem předchozím textu jsme se věnovali tomu, jak zabezpečit počítačovou síť. Seznámili jsme se se způsoby, jak zabezpečit router, jak správně nastavit bezdrátovou síť (wifi), jaké šifrování zvolit, jak lze regulovat obsah, který router do naší sítě propustí apod. Dnešní text věnujeme zabezpečení koncového zařízení, tj. samotného počítače, notebooku či tabletu, který pro přístup k internetovým službám používáme.

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**. Aktualizace především opravují chyby OS, prostřednictvím kterých by se do našeho počítače mohli dostat jak živí útočníci, tak různé druhy počítačových virů (malware).

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 systém Windows 10 obsahuje 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.). Poskytuje tak uživatelům minimální bezpečnostní standard bez nutnost instalovat další přídavné bezpečnostní aplikace.

5. Používejme antivirové programy

Přestože novější operační systémy obsahují integrovanou antivirovou ochranu, přesto je velmi dobré a žádoucí 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 - **Eset Family Security, Kaspersky Internet Security, AVG Internet Security, Avast Internet Security a Norton Security Deluxe**.

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

Tabulka: Základní druhy nebezpečného obsahu

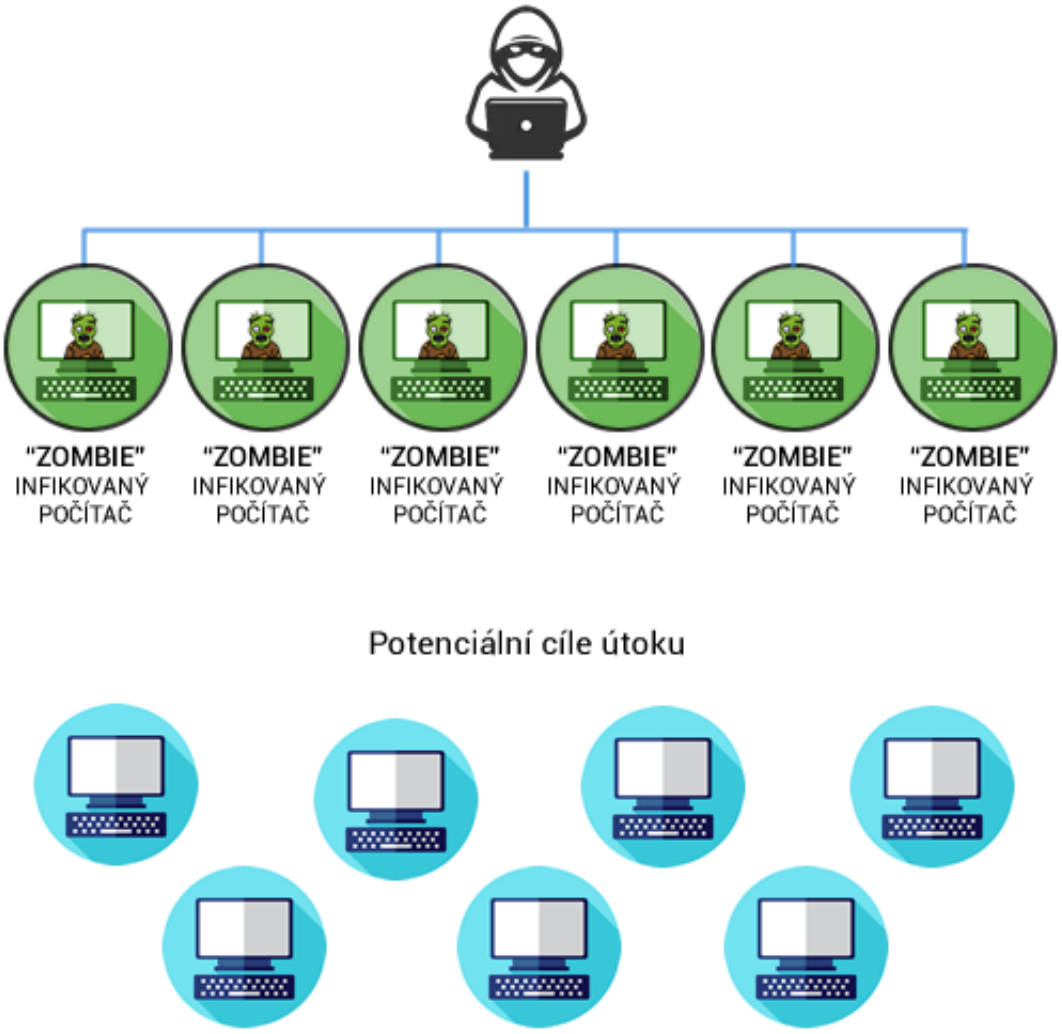
Druh nebezpečného programu	Co dělá
Počítačový červ	Nepotřebuje k šíření hostitelský program. Jakmile napadne počítač, začne své kopie bez vědomí uživatele posílat na další počítače a „prolézá“ tak internetem.
Trojský kůň / backdoor	Na první pohled vypadá jako užitečný program, nicméně umožňuje svému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



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. Pokud pak vytvoříme celou větu, nahradíme diakritiku číslicemi a dodáme speciální znak, je vyhráno. Tímto způsobem lze vytvořit silná a velmi bezpečná hesla. Hesla není nutné měnit příliš často, pokud je heslo silné, postačí klidně delší interval (třeba po roce, po dvou apod.). Příliš krátké intervaly změny hesla často vedou k vytváření slabých dobře zapamatovatelných hesel.

Pro účty, které se nachází 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 takového 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

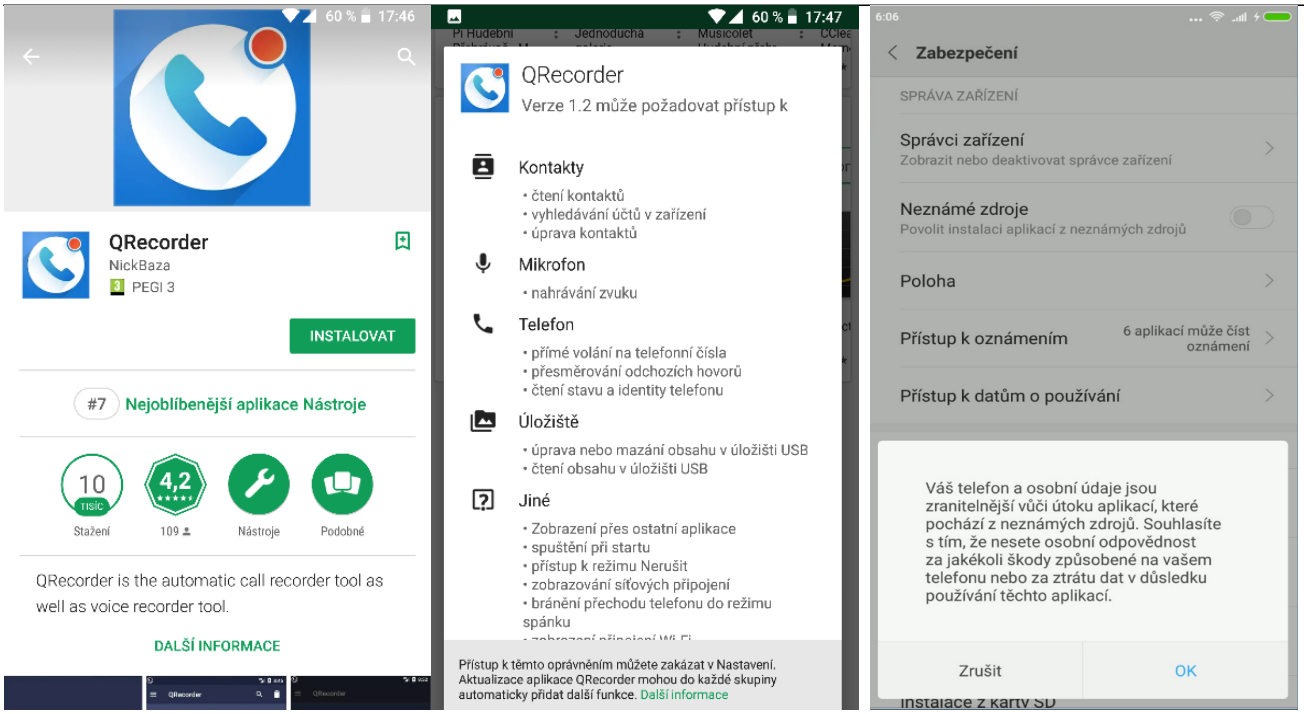
Stejná bezpečnostní opatření, která provádíme na běžném počítači

(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 jiného 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.

Obrázek: Aplikace QRecorder



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 software 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 z 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: Mark Zuckerberg má přelepenou webkameru

(Zdroj: Facebook.com, profil Marka Zuckerberga)

Aby se hackeři dostali k naší kameře např. 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 stali 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 postaveném 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 uživatele e-mailu, kteří podezřelé emaily tohoto typu ignorovali, nereagovali na ně, smazali je, označili za spam a v žádném případě nic neplatili.

Pro E-Bezpečí
Kamil Kopecký

Shrnutí

Použitá literatura

EMPEY, Ch. Jak si nastavit silné heslo. Avast, 2019. Dostupné z: https://blog.avast.com/cs/jak-si-nastavit-silne-heslo

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

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

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

KOPECKÝ, K. Jak zabezpečit domácí počítačovou síť. E-Bezpečí, roč. 4, č. 2, s. 44-48. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=1651

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

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

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

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

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

POTŮČEK, J. Tisíce Australanů čelí vydírání kvůli intimním záběrům přes webkameru. Eset – Dvojklik, 2016. Dostupné z:

https://www.dvojklik.cz/tisice-australanu-celi-vydirani-kvuli-intimnim-zaberum-pres-webkameru/

KOPECKÝ, Kamil. E-maily o tom, že pachatelé pomocí viru RAT získali vaše intimní materiály, jsou podvodné, jde o scam.. E-Bezpečí, roč. 3, č. 2, s. 45-47. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=1358

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

KOPECKÝ, K. Komentář: Zakázat mobilní telefon o přestávkách? E-Bezpečí, roč. 3, č. 2, s. 1-4. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=1316

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

*Poznámka: Text vyšel jako součást e-learningové opory **Základy počítačové bezpečnosti** v rámci projektu Kompetence leadera úspěšné školy (CZ.02.3.68/0.0/0.0/16_032/0008145).*