číslo 2 13.– 14. ledna 2018

Víkend DNES

Jde zdravě kouřit?

Nikdy nedávejte mobil z ruky

Mobilní telefon je klíč k vašim nejintimnějším datům. Nenechávejte ho ani na chvíli bez dozoru. Na jaké další technologické hrozby byste si měli dávat pozor a jak se účinně bránit **KYBERNETICKÝM ZLOČINCŮM?**

text: Tomáš Hečko / foto: archiv Karola Suchánka, Shutterstock

Češi podceňují bezpečí svých dat. Přitom takový únik informací dokáže člověku pořádně změnit život. Zažili to mnozí včetně Karola Suchánka, který si na tom vybudoval prosperující byznys. Dnes lidem radí, jak zabezpečit data v mobilu a počítači nebo jak se postarat o bezpečnost on-line připojených dětí.

Proč radíte s osobní digitální bezpečností?
Začal jsem s tím vlastně ve chvíli, kdy mi digitální data rozbila vztah. Dnes se tomu směju, ale tehdy mi to vtipné nepřipadalo.

Co se stalo?
Otec slavil sedmdesátiny, na víkend jsem odjel z Prahy. Přítelkyni nebylo dobře, zůstala doma. Když jsem jí z oslavy volal, slyšel jsem nahlas puštěnou hudbu. Přítelkyně tvrdila, že je u kamarádky. To se mi nezdálo. Přes iPhone a službu Přátelé jsem si ověřil, kde je. Byla doma. Takže jsem se přes telefon připojil k domácí kameře a všechno bylo jasné. Byla tam přítelkyně a můj župan, ale na někom jiném. Druhý den jsme se rozešli.

Vy máte doma dálkově ovládanou kameru?
Jsem IT maniak a pracoval jsem jako vývojář a programátor. Podobných hraček mám spoustu.

To jste ale výjimka. Takhle si nikdo do soukromí nahlížet nenechá.
To není pravda, i když mi to říkal každý, komu jsem se s touhle historkou svěřil. Když jsem začal vysvětlovat, kolik soukromých dat mají ve svém mobilu a počítači, začali se přátelé vždycky ptát, jak je udržet v bezpečí. A tak vlastně začala moje kariéra poradce v osobní digitální bezpečnosti.

Vždyť je to téma, o kterém se hodně mluví.
Možná teoreticky, prakticky se o to stará málokdo.

KAROL SUCHÁNEK (38)

- **Je absolventem cybersecurity programu** na Massachusetts Institute of Technology (MIT) v Bostonu.
- **Bezpečnostní software, který vyvinul v 16 letech,** vyhrál středoškolskou soutěž a dostal se až do běžného prodeje. Dnes o cybersecurity přednáší a organizuje semináře.
- **Baví ho** moderní technologie, běh, dobré jídlo a originální nápady. Je svobodný, bezdětný, žije v Praze.

Tak tedy prakticky. Co byste mi jako průměrnému majiteli počítače, chytrého telefonu a facebookového účtu poradil?
Především si uvědomte, že mobilní telefon je klíč, se kterým se kdokoli může dostat k vašim nejintimnějším datům.

Co si pod tím mám představit?
Cokoli, za co bychom se při zveřejnění mohli stydět nebo tím být vydíratelní. Nemusí to být rovnou nahota, ale třeba i záběry z vydařeného večírku. A také cokoli, co ohrozí soukromí a bezpečnost. Nejčastěji uložená hesla, přístupy k účtům (banky, sociální sítě), podrobnosti o bydlišti. Nikdy nedávejte telefon z ruky a nenechávejte ho ani na chvíli bez dozoru. Nikdy!

Dobrá. Pravidlo číslo jedna – mobil nedávat z ruky. Co dál?
Tady se dostáváme k hlavní zásadě osobní digitální bezpečnosti. Mezi útočníka a naše data musíme dávat co nejvíc vrstev ochrany. Aby to vypadalo jako „cibule" – když se povede sloupnout jednu slupku, vyskočí na útočníka další. Takže pro případ, že ochrana číslo jedna padla a mobil jste ztratil, měl byste ho zabezpečit. Mohu se zeptat, jak svůj mobil odemykáte?

Gestem.
To není tak dobrá volba. Gesto se dá lehce zapamatovat, pokud ho někdo zahlédne. A prst zanechává při opakovaném zadávání na displeji stopu, ze které může útočník gesto odvodit. Minimálně si změňte gesto na takové, při kterém po některých přímkách jezdíte víckrát. Takové se nedá z otisku na displeji jednoznačně určit. A raději přejděte na nejméně šestimístný číselný kód.

Mohu telefon i počítač odemknout také otiskem prstů.
Tady záleží na tom, jak citlivá data v telefonu a počítači máte. Pro běžného uživatele

jsou otisky prstů celkem dobrá volba. Pokud by se ale kvůli těm datům vyplatilo vás přepadnout, uspat a pak zařízení odemknout, pak je to spíš bezpečnostní riziko.

Jaká je další vrstva zabezpečení telefonu?
Nastavte si telefon tak, aby po několikanásobném zadání chybného hesla smazal všechna data. Tím používání telefonu případným zlodějům dále zkomplikujeme a zvýšíme ochranu svých dat. Pořád musíme myslet na to, že neexistuje jedno zázračné zabezpečení, ale že cílem je přístup k našim datům kombinací různých opatření co nejvíc znesnadnit.

Takže útočník zadal chybné heslo a k mým datům se nedostal. To je fajn, ale data teď nemám ani já.
Máte samozřejmě zapnuto zálohování dat. Ukládáte si je buď do nějakého důvěryhodného cloudu, nebo na svůj počítač, nejlépe na externí harddisk. A máte vše dobře zabezpečeno – je tam antivirus, firewall, aktualizovaný systém, zabezpečení silným heslem a nejlépe ještě zašifrovaný disk. Přijdete jen o data za pár dnů nebo hodin – od poslední zálohy. Samozřejmě i záložní disk vám mohou ukrást. Musíte zvažovat rizika. Žádné zabezpečení není stoprocentní.

Ještě poradíte nějaké triky s chytrým telefonem?
Zapněte si funkci Find My iPhone nebo u Androidu Find My Device. V případě, že vám telefon ukradnou a zloděj jej zapne, můžete jej na dálku lokalizovat a případně z něj smazat vaše data. Navíc se telefon s touto funkcí stává bezcenným, protože se později nedá prodat. Žádný překupník nechce přístroj, který může původní majitel vysledovat. A pro jistotu si také opište a uschovejte IMEI přístroje a účtenku. IMEI je číslo jedinečné pro každý telefon. Když s účtenkou a IMEI nahlásíte policii krádež, můžete telefon nechat zablokovat.

Mám tři malé děti. To nejstarší, osmileté, zdědilo po mámě laptop, našetřilo si na tablet a pošilhává po chytrém telefonu. Jak vyřešit bezpečnost?
Rodiče si často myslí, že pro vyřešení problému osobní digitální bezpečnosti dětí stačí koupit nějaký zázračný program. Tak to není. Nejdůležitější je děti vzdělávat a o rizicích mluvit. Samozřejmě tak, aby to odpovídalo jejich věku.

Co všechno dětem hrozí?
Rodiče se nejčastěji obávají konzumace nevhodného obsahu, především pornografie a násilí. Těch nebezpečí je ale víc a všechna souvisejí s nepromyšleným sdílením soukromí dítěte. Dítě se může stát terčem kybernetické šikany. Obvykle od vrstevníků. Ale mohou je obtěžovat také dospělí nebo může být terčem kybergroomingu. To znamená, že se někdo pokusí dítě zmanipulovat tak, aby se vystavilo nebezpečí. Obvykle se je snaží vylákat na schůzku.

To zní jako noční můra.
Ano, je to riziko. Ale i zdánlivě nevinné sdílení fotografií může nakonec pro dítě znamenat trauma. Data na webu zůstávají navždy. Dítě už nyní tvoří svou digitální stopu a za pár let nemusí být z některých veřejně dostupných informací nebo fotografií tak nadšené jako dnes. Nad tím by měli přemýšlet i rodiče ve chvíli, kdy zveřejňují cokoli ze soukromí dětí.

Jsou ještě nějaká další rizika?
Ano, děti mohou, stejně jako dospělí, naletět phishingu, tedy situaci, kdy jim někdo podvrhne falešnou stránku a ony nevědomky vyzradí své přihlašovací údaje. Děti také často mívají lehce odhalitelné odpovědi na bezpečnostní otázky, používají jednoduchá a všude stejná hesla a nemívají zapnuto dvoufaktorové ověřování. To vše musíme hlídat.

A co tedy doporučujete?
V první řadě s dítětem všechny hrozby otevřeně probrat. Nezakazovat, spíš ukázat, co všechno se může stát. Zakázané ovoce chutná nejvíc, to platí i na internetu. Dítě je třeba naučit, že na internetu se může kdokoli vydávat za kohokoli a že nemůže důvěřovat lidem, které osobně nezná. Že existují meze, co se sdílení soukromí týče. Že stejně jako některé věci neukazujeme každému na potkání, neděláme to ani na internetu.

Co sociální sítě nebo e-mail?
E-mail dítěte by měl zůstat co nejdéle pod stoprocentní kontrolou dospělého. Tedy rodič by do něj měl mít přístup a dítě by to mělo vědět. Rodič by toho neměl zneužívat a vložit se do věci jen v případě, kdy opravdu hrozí nebezpečí. Sociální sítě jako Facebook nebo Instagram by děti do 13 let neměly vůbec používat. Tedy podle americké legislativy. Tlak vrstevníků je ale ohromný. Jako dobrý kompromis mi připadá účet na Instagramu, který lze nastavit jako neveřejný, a dítě tady sdílí jen s ověřenými příbuznými a kamarády.

Jak dítě naučit obraně proti dospělým predátorům?
Je to věc výchovy. Dítěti je třeba vštípit několik zásad. Nikdy nikomu cizímu neposílat jakékoli informace o rodině nebo fotografie. Kdykoli někdo cizí dítě vystraší, žádá o pomoc, vyhrožuje, snaží se je dostat do časového stresu, je třeba přerušit konverzaci a říci o tom rodiči. Klidně si s dítětem zahrajte hru na teoretické situace, které mohou nastat, a ptejte se jej na správnou reakci. Ale hlavně – pokud se cokoli stane, musí dítě vědět, že se s jakýmkoli problémem může svěřit rodičům a že ti mu pomůžou. Nesmí se bát, že sklidí kritiku.

Ale co když se někdo cizí vloudí v přestrojení za známého?
Je třeba dítě naučit držet se zásady, že nové přátele přijímá jen po předchozí dohodě nebo telefonickém ověření. Dobrá příležitost jsou třeba oslavy, kdy se rodina a přátelé fyzicky potkají. Dítě musí

vědět, že by si mohlo omylem mezi přátele přidat cizího člověka – jmenovce svého kamaráda. A mělo by vědět i to, že i účet někoho blízkého se může začít chovat nebezpečně, protože může být napadený.

Co nevhodný obsah?
Zapněte rodičovský zámek. To lze jak ve Windows, tak na iPhonu i telefonu s Androidem. Podobnou službu nabízejí také antivirové programy. Dalším krokem může být nastavení dětského vyhledávače, například www.kiddle.co. A pokud máte staršího potomka, který by chtěl takovou ochranu obejít, můžete na domácí wi-fi síti nastavit službu OpenDNS. Ta je zdarma a zabrání přístupu k nevhodnému obsahu každému připojenému zařízení.

Jak se vlastně Češi chovají ke svým datům?
Nic moc, řekl bych. Výjimku tvoří jen lidé, které k digitální bezpečnosti systematicky vedou v zaměstnání. Přitom vlastní data jsou takové rodinné stříbro. Jenže spousta chytrých a odpovědných lidí dělá ty nejzákladnější chyby. Neuvědomují si, o jaké tragédie si koledují. Poznal jsem lidi, kteří v jediném okamžiku přišli o měsíce a roky práce, stali se vydíratelnými, zničili si soukromý nebo pracovní život. Jen proto, že se ke svým datům ve virtuálním světě chovali tak, jak by je to ve skutečnosti nikdy nenapadlo.

Mezi kybernetického útočníka a naše data musíme dávat co nejvíc vrstev ochrany. Aby to vypadalo jako „cibule" – když se povede sloupnout jednu slupku, vyskočí na útočníka další.

Kdybyste měl říci pár jednoduchých zásad, tak kterých se držet?
Opakuje se to pořád dokola: základem všeho je aktualizovat si v počítači a v telefonu operační systém. Neignorujte aktualizace, přinášejí opravy bezpečnostních chyb, které se v poslední době objevily, a občas i nové funkce. Jak zranitelné jsou neaktualizované systémy, ukázal v květnu vyděračský virus, který napadal po celém světě neaktualizované počítače. Pak je také správné data na disku zašifrovat – u Windows je na to BitLocker, máte-li Mac, hledejte funkci FileVault. Další samozřejmostí by měl být antivirový program na počítači i v mobilu. I verze zdarma udělají dobrou práci.

To snad dělá každý.
To byste se divil! Podobně je to i s hesly. Málokdo používá k přístupu k datům a službám dlouhá, rozmanitá a neopakující se hesla. Přitom silná hesla a zapnuté dvoufázové ověřování totožnosti jsou základem osobní digitální bezpečnosti.

Hesel mám hodně, pamatuje si je za mě můj prohlížeč.
Chyba! Dostane se k nim kdekdo. Doporučoval bych mnohem větší opatrnost. Stáhněte si „password manager" – softwarový trezor. Nemusíte si pak pamatovat všechna hesla, stačí znát jedno hlavní. Nebo se za pár stokorun dají pořídit off-line trezory, například Passwords FAST. V nich můžete mít data uložena úplně mimo internet, v kapse nebo v kabelce.

Co dalšího doporučujete?
Bezpečnostní díru dnes představují domácí routery. Některé mají z továrny nastavené velmi jednoduché heslo, je lehké je prolomit a odposlouchávat veškerý váš datový provoz. Změňte si heslo na routeru. Ještě dnes. A v routerech aktualizujte software.

Když to všechno shrneme, jmenujte prosím tři klíčové rady.
Už jste je jistě mnohokrát slyšeli, ale zkuste je konečně dodržovat. Pravidelně svá data zálohujte. Neklikejte bezhlavě na všechno, co vám přijde pod ruku – na internetu, na sociálních sítích ani v mailu. A naučte to všechny vaše blízké.

vikend@mfdnes.cz