ISSN 2336-7989

Innovation

Velký investiční průvodce

3 2017 cena 149 Kč

Žijeme jen jednou, ale data navždy.

TAK ZNÍ HESLO KAROLA SUCHÁNKA, CYBERSECURITY SPÍKRA

s. 14

INVESTICE → S. 38

Kryptoměny: Bitcoin

TECHNOLOGIE → S. 68

IFA: veletrh spotřební techniky

INVESTICE → S. 26

Jak investuje dolarový milionář?

STYL → S. 50

Odpočinek v Asii: **Indonésie**

Informační technologie jsou pro Karola Suchánka koníčkem už od střední školy. Bezpečnostní software, který vyvinul v šestnácti letech, nakonec vyhrál středoškolskou soutěž a dostal se až do běžného prodeje.

Žijeme jen jednou, ale data zůstávají navždy

Ještě před pár lety by slovo cybersecurity znělo pro většinu z nás jako pojem z hollywoodského filmu. Co cybersecurity znamená, jaká nebezpečí na nás číhají a jak se jim nejlépe bránit? Na to jsme se zeptali Karola Suchánka, který se na tuto problematiku specializuje.

TEXT Zuzana Veberová **FOTO** Archiv Karola Suchánka

V čem může být pro nás internet nebezpečný? Proč bychom si měli dát pozor?

Už dávno neplatí, že internet je „jen internet". Internet se stal součástí našeho každodenního života. Dnes internet nejen odráží reálný svět, ale naopak se i virtuální obsah promítá do našich životů. Tento vývoj byl možná až příliš rychlý, a tak si mnoho lidí často ani neuvědomuje, co všechno na síti s ostatními sdílí. Často to mohou být kromě otravných fotek jídla i citlivé údaje nebo fotky, které si může každý nejen prohlídnout, ale i uložit a potom s nimi nakládat zcela po svém. A to i způsobem, který se nám nemusí líbit nebo nás může dokonce rovnou poškodit.

Můžete uvést nějaký příklad?

Poměrně klasickým příkladem jsou různé podvodné maily, které po vás chtějí například čísla vašich kreditních karet nebo hesla k různým účtům.

Data mají na černém trhu velkou cenu a obchoduje se s nimi úplně běžně. Točí se v něm více peněz než v drogách.

Co se týče mladší generace, tam se jedná například o fotografický materiál, který je velmi citlivý nebo je intimní povahy a kterým pak manipulátoři oběť vydírají.

Poměrně aktuálním a častým projevem neopatrnosti jsou například veřejně sdílené fotky letenek, kde i z drobných údajů na kusu papíru může šikovný podvodník velmi rychle získat přístup do vašich rezervací, kde máte e-mailovou adresu, číslo pasu, datum narození a může vám lehko změnit sedadlo, jídlo nebo zrušit letenku na cestu zpátky. Pouze ze zábavy, jen tak. Vám to ale vtipné na druhém konci světa asi nepřijde. Nicméně vzhledem k tomu, že je cestování stále oblíbenější a lidé své zážitky na sociálních sítích sdílejí víc a víc, budeme se s podobnými zločiny setkávat stále častěji. Informaci, že váš domov je aktuálně prázdný, může taky využít zloděj a přijít na „neohlášenou návštěvu". A to nechcete. →

U nás si lidé na sociální sítě například napíší cokoli je napadne. A to často i velmi citlivé věci, pořád máme za to, že „je to jen internet“.

Jak se takovým neštěstím vyhnout?

Kdysi mi někdo říkal, že nejlepší způsob, jak se vyhnout nějakému nebezpečí je být co nejdál od něj. To může fungovat třeba v případě požáru nebo tornáda. Z internetu ale jen tak neodejdete, stejně jako jen tak neodejdete ze společnosti. Vyměnit bezpečí za život poustevníka pro většinu lidí není příliš lákavé.

Nejlepším řešením je dávat si pozor. Mít určitou prevenci a bezpečnostní páky, které vám budou pomáhat ochránit svá citlivá a soukromá data. Jakmile je jednou něco venku, je to většinou venku napořád. Cesta zpátky bývá náročná a někdy bohužel nemožná. Důležité je tedy podniknout co nejvíce kroků, aby se věci ven nedostaly.

Lidé si naivně myslí, že nejsou zajímaví, pro cyber kriminalitu jsme ale zajímaví všichni. Představte si to jako ryby v moři, útočníci zkouší, nechytne se jedna ryba, chytne se druhá. Data mají na černém trhu velkou cenu a obchoduje se s nimi úplně běžně. Toto odvětví je největší ilegální byznys a točí se v něm více peněz než v drogách.

Napadá vás nějaký způsob, jak by se třeba například někdo mohl dostat k mému heslu dejme tomu na Facebook?

Pokud pomineme klasický způsob, tedy že z vás někdo heslo vymámí takzvaným „social engineeringem“, obvykle podvodným mailem nebo nějakou manipulací, jsou poměrně nebezpečná i hesla uložená v prohlížeči. Pokud se například někdo dostane k vašemu počítači, je pak jisté, že se tímto způsobem jednoduše dostane do vašeho účtu. Ale taky mu stačí zhruba dvě minuty ve vašem prohlížeči, aby dokázal heslo dostat z jeho zašifrované podoby, někam si ho zkopíroval a pak se do vašich účtů už dostal odkudkoli. Takže i tahle zjednodušující vymoženost, kterou všechny internetové prohlížeče disponují, může vést ještě k velkým problémům. Určitě nedoporučuji prohlížet si své účty na veřejných počítačích, třeba na letišti nebo na hotelu. A už vůbec ho nikomu nesdělovat. Naivní důvěra se v on-line světě zkrátka nenosí. Všude, kde to lze, zapněte si dvoufaktorové ověřování. Dobře to znáte z internetového bankovnictví, je to číselný kód, který vám jako druhý faktor ochrany přijde přes sms na váš mobilní telefon.

Pokud máte jedno jediné heslo, které používáte ke všem účtům, pak během krátké chvíle můžete přijít nejen o peníze, ale i o svou identitu. Mělo by platit základní pravidlo, co účet, to unikátní heslo. Také je fajn hesla někdy změnit, třeba dnes večer.

Jestli tomu dobře rozumím, je tedy lepší mít více různých hesel a pokud možno je nemít uložená v prohlížeči.

Přesně tak. To je asi naprostý základ. Na svých přednáškách často používám přirovnání, že heslo je jako klíč a jak máme od každých dveří vlastní klíč, tak bychom měli mít do každého účtu odlišné heslo.

Ale hesel účtů všech možných služeb má dnes člověk i desítky. Kdyby si je měl všechny pamatovat, musel by se zbláznit...

Vůbec není potřeba se zbláznit. Existuje řada aplikací, ve kterých si svoje hesla můžete bezpečně uložit. A to on-line nebo off-line. Dnes je ani nemusíte mít uložená na počítači, stačí si pořídit úložiště, takový trezor na hesla, který můžete nosit s sebou a kdykoli se do něj přes jedno jediné řídicí heslo podívat a svá hesla si najít. Dobrým příkladem je passwordsFAST, který stojí jen pár stovek a uloží vám až 125 hesel. Je malý, vejde se do kapsy a je velmi bezpečný. Stačí si opravdu pamatovat jedno heslo. Je to elegantní a velmi praktické řešení, které ihned eliminuje celou řadu bezpečnostních rizik.

Co je hlavní výhoda takového zařízení?

Především to, že je off-line. Není připojené k žádné síti, nesdílí s nikým žádná data, nelze z něj data vydolovat nějakým sofistikovaným způsobem. Musíte prostě znát heslo, jinak máte smůlu. Běžné trezory mají tu nevýhodu, že je nelze nosit s sebou (nebo je to aspoň velmi nepohodlné a nepraktické), tohle zařízení se vám vejde do kapsy v saku nebo kalhotách.

Že si lidé na svá data nedávají pozor lze vidět skoro každý týden, neustále čteme o nějakém úniku dat. Čím to je, že takovéto zprávy nejsou pro lidi dostatečným varováním?

Možná je to taky tím, že si lidé ještě nedokážou úplně představit, co všechno jsou citlivá data. U nás si lidé na sociální sítě například napíší cokoli je napadne. A to často i velmi citlivé věci, pořád máme za to, že „je to jen internet“.

Jenže opak je pravdou. Žijeme jen jednou, ale data zůstávají navždy. Skoro všechno lze zpětně

PasswordsFAST, který stojí jen pár stovek a uloží vám až 125 hesel. Je to elegantní a velmi praktické řešení, které ihned eliminuje celou řadu bezpečnostních rizik.

dohledat, zkopírovat, šířit. Například u většiny firem je dnes zvykem, že si jejich personalisté prohlédnou sociální sítě kandidátů o zaměstnání. A co všechno tam mohou najít, že. Něco, co se vám může zdát, jako nevinná legrace může být bez kontextu pro někoho zcela nepřijatelné a odporující firemní kultuře zrovna vašeho vysněného zaměstnavatele. Může jít třeba o rasistické tweety, fotomontáže založené na černém humoru nebo vaše vlastní fotky, na kterých můžete být ve velmi nedůstojných situacích. A neplatí to jen pro dospělé lidi a jejich kariéru, myslet by na to měli především mladí, kteří na své sociální sítě v nevinné lehkovážnosti dávají spoustu věcí, o kterých zatím ani nemohou tušit, že se jim jednoho dne mohou vrátit.

V posledních letech jsme byli svědky toho, že kvůli uniknutému videu nebo ne zrovna nejšťastnější reakci na Facebooku, přišla nejedna osoba o své zaměstnání. Sociální sítě jsou jako lavina a netřeba je podceňovat.

Co dáváte na internet, to tam také zůstane. A jednoho dne to přiletí zpátky jako bumerang. Fotky, komentáře, hesla, data, všechno. Není to jen internet, je to fenomén, který se nejen do našich životů prolnul, ale častokrát ho z velké části i překrývá. Zařídit si bezpečnost na internetu znamená zařídit si bezpečnost v životě.

Jedinci tedy dělají chyby. Dělají je ale i velcí hráči? Instituce, korporace, firmy?

Ano, často. Nejnověji například jedna z třech největších amerických úvěrových společností, Equifax. Té kdosi ukradl údaje o 143 milionech klientů.

Než společnost útok odhalí, uběhne v průměru až 87 dnů. Zarážející je i fakt, že až 71 % napadnutých společností útok neodhalí sama.

Jeden z velkých českých on-line obchodů zase nedávno oznámil, že mu byla ukradena data 1,3 milionu uživatelů. Jestliže se v takových případech nemůžete zcela spolehnout na bezpečnost ze strany provozovatele služby, ať už je to státní instituce nebo firma, musíte se spolehnout více sami na sebe. Nepoužívat stejná hesla, neklikat na podezřelé odkazy, nenechat se nachytat útočníky, kteří z vás chtějí vylákat informace.

Co byste doporučil zaměstnavatelům?

Nejdůležitější je systematicky zvyšovat povědomí všech pracovníků firmy o cybersecurity. Zaměstnanci by se měli naučit jednoduché a jasné zásady, které budou vždy dodržovat a následně je namátkou a pravidelně testovat, například phishingovým e-mailem, telefonátem či podstrčením USB klíčem. Část bezpečnostních útoků přichází zevnitř firem, od lidí, kteří například odcizí korporátní data, když společnost opustí nebo jsou vyhozeni. Samozřejmě je třeba ošetřit pracovněprávní vztahy se zaměstnanci tak, aby pokrývaly i rizika cybersecurity a v případě, že se něco stane, daly firmě do ruky silný nástroj pro minimalizaci škod.

Než společnost útok odhalí, uběhne v průměru až 87 dnů. Zarážející je i fakt, že až 71 % napadnutých společností útok neodhalí sama.

Čeká Česko v ohledu cybersecurity nějaká renesance nebo aspoň zlepšení situace?

Nevyhnutně. Jednoho dne to možná bude chování stejně zažité, jako jsou dnes například pravidla silničního provozu. Jenže k tomu nám ještě pořád nějaký kus chybí.

Na trhu je ale už nyní spousta kvalitních aplikací a zařízení, které mohou zabezpečit vás a vaše on-line aktivity. Nejlepší ze všeho je ale zkrátka být před útočníky o krok napřed a začít už nyní – u sebe. Pokud má kdokoli zájem, může se například objednat na mou přednášku o cybersecurity, na které se dozví, jak na to.

Začněte u sebe, používejte více hesel a dávejte si jednoduše pozor. Šiřte základní povědomí o tom, že cybersecurity je důležitá pro každého z nás. Je určitě lepší být dnes opatrný, než zítra plakat. ×

Karol Suchánek

Informační technologie jsou pro Karola Suchánka koníčkem už od střední školy. Bezpečnostní software, který vyvinul v šestnácti letech, nakonec vyhrál středoškolskou soutěž a dostal se až do běžného prodeje. První část profesionální kariéry pracoval na vývoji software a získal Bakaláře Informačních technologií na Univerzitě Konštantína Filozofa v Nitre a později také MBA na University of New York in Prague. Jeho zájem o technologie ho přivedl k cybersecurity problematice, o které dnes přednáší a organizuje semináře pro širokou veřejnost i firmy. Je absolventem speciálního cyber-security programu na Massachusetts Institute of Technology (MIT) v Bostonu. Více se o něm dozvíte na webu www.karolsuchanek.com.