profi HR

září / 2017

Psychopat na pracovišti

Slashies

PROJEKTOVÉ ŘÍZENÍ PO ČESKU ANEB „DĚLÁME“ PROJEKTY

TÝM SLOŽENÝ Z HVĚZD NEMUSÍ VYHRÁT

KDO SI ZAMĚSTNANCE VÍCE HÝČKÁ?

Direktivní přístup u nás nemá místo,

říká Martina Brožová z JetBrains

Naše data nás přežijí

Cybersecurity, před několika lety širší veřejnosti nepříliš známý pojem, dnes stále důležitější součást našich běžných životů. Měli bychom se chránit, ale často ani netušíme před čím, natož jak. O tom, co cybersecurity znamená a jaká rizika číhají na každého z nás, jsme se bavili s Karolem Suchánkem, který o problematice bezpečnosti na internetu přednáší.

Proč bychom se vůbec měli na internetu chovat opatrně?

Říkávám, že my sice žijeme jen jednou, ale naše data tady budou navždy. Málokdo si uvědomuje, že cokoli jednou sdílí na internetu, to přestává mít pod kontrolou. A může to být fotografie, videozáznam, nebo třeba jen nešťastně formulovaný tweet. To vše si rázem žije vlastním životem a pokud je to informace, která je použitelná proti vám, máte jednoduše smůlu. Na internetu nedostanete druhou šanci. A problém se pak může vracet znovu a znovu. Internet nezapomíná.

Takže jedinou možností, jak se vyhýbat problémům, je prevence?

Přesně. Napravování škod bývá náročné na čas, energii i peníze. A často není úplná náprava ani možná.

Co se vlastně může člověku na internetu přihodit?

Můžete třeba přijít o peníze. O tomto problému se naštěstí, především díky úsilí finančních institucí, docela mluví. Lidé si uvědomují, že například heslo od online účtu, nebo veškeré podrobnosti týkající se platební karty, je třeba uchovávat v tajnosti a nesvěřovat je vůbec nikomu. Ať se protistrana tváří sebeseriózněji.

Takže stačí chránit přístupové údaje k penězům?

Zdaleka ne. Nemusíte přijít jen o peníze. Máte spoustu dalších cenností, které stojí za to chránit. Vaše pověst, soukromí, soukromí vašich blízkých, osobní nebo pracovní data. To všechno jsou hodnoty, které mohou mít penězi nevyčíslitelnou cenu.

Chráníme si je?

Ne.

Proč?

Většinou je za tím nevědomost. Často si lidé ani neuvědomují, že zacházejí s něčím, co je, nebo může být, citlivá informace. Divili byste se například, co všechno mají lidé uloženo ve svém více či méně nechráněném chytrém telefonu. Důvěrné pracovní dokumenty, lechtivé obrázky nebo videa, zneužitelné podrobnosti ze soukromého života. Často je důvodem také pohodlnost, třeba když zadáváte do všech aplikací stále stejné heslo.

Nejdůležitější je systematicky zvyšovat povědomí všech pracovníků firmy o cybersecurity. Zaměstnanci by se měli naučit jednoduché a jasné zásady, které budou vždy dodržovat.

Kdo by si ty desítky hesel pamatoval…

Existují programy, ve kterých můžete mít svá hesla uložena. Nebo si je dokonce můžete nosit s sebou, zcela mimo internet. Stačí si pořídit off-line úložiště, „trezor" na hesla, jako je například Passwords Fast. To je investice několika stokorun, díky které můžete chránit hodnoty o několik řádů vyšší. Že se vyplatí v tomto ohledu přemýšlet, ukázal nedávný případ, kdy jeden z velkých českých online obchodů oznámil, že mu byla odcizena hesla 1,3 milionu uživatelů. Pokud se to stane a vy jste máte stejné heslo třeba na sociálních sítích, můžete přijít o množství dat, kontakty, vybudovanou komunitu. To je dost velká cena za lenost.

V čem jsou Češi ještě lehkovážní?

Vyměňovat si se svým současným partnerem erotické snímky nebo videa může být v první chvíli docela šťavnatá zábava, problém ale nastane ve chvíli, kdy se rozejdete. Pomsta zhrzeného partnera je dost obvyklý scénář, jak se na veřejnost mohou dostat fotografie nebo videa, ze kterých rozhodně nebudete mít radost. Nebo fotografie dětí. Dnes mnoho rodičů sdílí fotografie svých dětí hlava-nehlava a neuvědomují si, že tím vytvářejí dítěti digitální stopu, o kterou jednoho dne třeba nebude jejich potomek příliš stát. Opět to připomínám, data jsou věčná.

Máte nějaké ponaučení pro zaměstnavatele?

Na jednu stranu je současná situace pro personalisty výhodná. Protože často můžete relativně lehce získat velmi ucelený přehled o osobnosti kandidáta – o jeho životních postojích, rodinné situaci, koníčcích, ale třeba i financích. Já často apeluji na to, aby lidé pohlíželi na informace, které o sobě vypouštějí do

Foto: Archiv autora

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 Nitře a později také MBA na University of New York in Prague. Jeho zájem o technologie ho přivedl k problematice kybernetické bezpečnosti, 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.

světa, i z tohoto úhlu pohledu. Říkám o sobě něco, co chci, aby měl na stole personalista rozhodující o mém přijetí do zaměstnání? Na straně druhé je ale současná situace pro zaměstnavatele i nebezpečná.

V čem?

Protože podobně lehkovážně, jako se svými daty, zacházejí lidé často i s těmi firemními. Nevidí v tom větší rozdíl. A to může být zdrojem problémů. Často velkých problémů.

Co byste zaměstnavatelům doporučil?

Nejdůležitější je systematicky zvyšovat povědomí všech pracovníků firmy o cyber-security. Zaměstnanci by se měli naučit jednoduché a jasné zásady, které budou vždy dodržovat a následně je namátkou a pravidelně testovat, například phishingovými e-mailem, telefonátem či podstrčeními USB klíčem. Pak samozřejmě není od věci být velmi opatrný ohledně zaměstnanců IT oddělení. Část bezpečnostních útoků přichází zevnitř firem, od lidí, kteří právě spravují firemní IT, například odcizí korporátní data, když společnost opustí nebo jsou vyhozeni. Samozřejmě je třeba ošetřit pracovněprávní vztahy se zaměstnanci tak, aby pokrývaly i rizika cyber-security a v případě, že se něco stane, daly firmě do ruky silný nástroj pro minimalizaci škod.

Existuje v oblasti cybersecurity něco, o čem se u nás zatím příliš nemluví?

Možná to nespadá přímo do oblasti bezpečnosti, ale úzce to souvisí s vlastností internetu, ke které se stále vracím – že totiž internet nezapomíná. Pokud vám záleží na vaší pověsti, měli byste se na internetu ovládat a chovat slušně. Libovolné, i nezamýšlené faux pas se může proměnit ve velký problém. Před několika lety se proslavil případ, kdy jedna neznámá americká manažerka odeslala před mnohahodinovým letem do Jihoafrické republiky nepříliš chytrý a velmi rasistický tweet a vypnula telefon. Když jej na letišti v Kapském Městě opět zapnula, zjistila, že shodou náhod jejich dvanáct slov naštvaně retweetovaly tisíce lidí, že se stala na chvíli veřejným nepřítelem číslo jedna a její profesionální kariéra právě skončila. Pokaždé, když něco umisťujete na internet, může se vám stát totéž. Přemýšlejte.

Jak vidíte budoucnost cybersecurity?

Před pár lety si nikdo nepředstavoval, že internet bude zcela přirozeně používat doslova každý – malé děti, senioři, lidé, kteří jinak s IT technologiemi nemají nic společného. Naučili se to a jsou v tom stále lepší. S ochranou vlastních údajů, opatrností a dodržováním bezpečnostních pravidel to bude podobné. Postupně je začneme přirozeně dodržovat úplně všichni, bude to samozřejmé. Bude to ale ještě stát úsilí, čas i peníze. ✕ **red**