

# Kryptologie a nové technologie

## Vánoční blahřečení heslu 123456

Bezpečnostní výzkumník, který se dostal k heslům 10 000 e-mailových účtů na Hotmailu, se svěřil, že nejčastějším heslem obětí byly řetězce 123456 a 123456789. Hesla byla získána phishingem; uvízla zde i hesla silná (6 %), která obsahovala kombinaci písmen, číslic a speciálních symbolů.

Používání těchto hesel je ale pro určité účely dostačující. Nežijeme ve vakuu a naše e-maily jsou chráněny stejně jako listovní tajemství v klasických dopisech. Kdo naruší listovní tajemství nebo zneužije přístupové údaje, páchá trestný čin. Ani poskytovatel e-mailové schránky nesmí narušit listovní tajemství. Jestliže si tedy elektronickou poštou posíláte nedůležité informace (nezpeněžitelné útočníkem), je ochrana heslem typu 123456 lepší než při použití hesla qsu4A5@2K15sd zvoleného také pro banku. Podobné úvahy platí o Facebooku apod. Není-li co chránit, je vhodnější heslo raději slabé než takové, které prozrazuje heslo k bankovnímu účtu nebo metodu jeho tvorby. Slabé heslo lze používat pro e-mailovou schránku, jsou-li důležité soubory před odesláním zašifrovány silným klíčem a kvalitním programem. Jestliže je však heslo 123456 používáno i pro přístup k bankovnímu kontu, to pravděpodobně bude jednou vykradeno. Útočníci získávají přístup k takovým účtům plošně, zejména phishingem, tudíž nepomůže výmluva typu „kdo by se staral o můj účet, stejně nikdo nezná jeho číslo“. Zřejmě takových ignorantů je stále hodně, protože jen v USA v roce 2007 takto utrpělo škodu asi 3,5 milionu uživatelů a v roce 2008 již pět milionů, a to v průměrné výši 351 dolarů.

## Bezpečnost IT je zákonitě podružná

Internet není bezpečné médium, nebyl takto od počátku stavěn, a proto v současné podobě nikdy bezpečný nebude (možná, že se za deset let začne vytvářet jiný „internet“). Jako běžné lidé dokonce přijali na hlavu postavené pravidlo pro záplatování operačního systému a aktualizaci antivirových databází: „abychom byli chráněni před útoky z internetu na náš počítač, je nutné náš počítač na internet připojit“ a navíc umožnit, aby se někdo neznámý hrabal v našem obranném systému. Ještě před několika lety se to dělalo správně a bezpečně off-line prostřednictvím aktualizací CD, ovšem distribuce kompaktních disků byla pomalá a drahá, a tak nastoupila pohodlnější a rizikovější cesta on-line.

## Bezpečnost IT je adekvátní potřebám

Bezpečnostní problémy, které s sebou nesou nové technologie, jsou nutně odsouvány do pozadí jejich přínosy a lidé se smiřují s novými paradoxy. V době, kdy byli poučeni o nebezpečích internetu, začali ho masivně používat pro osobní i firemní bankovníctví. Zatím tahle hra vychází velmi dobře ve prospěch přínosů, ovšem nelze zase příliš riskovat. Jinými slovy,

**Tabulka 1**  
Nejpoužívanější hesla

1.	123456
2.	123456789
3.	alejandra
4.	111111
5.	alberto
6.	tequiero
7.	alejandro
8.	12345678
9.	1234567
10.	estrella

je možné používat nebezpečné technologie (když jsou užitečné), ale je nutné si být vědomi rizik a odpovídajícím způsobem se chránit. Jedna poškozená majitelka malého českého hotelu tato rizika podcenila, nebo pravděpodobněji o nich neměla tušení, a tak přišla o 1,5 milionu, což bylo pro její hotýlek likvidační a pro ni samu životní tragédie. Asi jí nebude velkou útěchou, že škody způsobené prostřednictvím internetu mohou být vysoké, ale nikoliv nejvyšší. Automobilismus je oproti informačním technologiím stokrát nebezpečnější, a přesto si k němu lidé vybudovali vztah. Víme o rizicích, žijeme s nimi. Kdo se nechrání, nebo přímo riskuje, může zaplatit cenu nejvyšší. Zaplatit za cizí chyby může dokonce i ten, kdo se chrání, za nic nemůže a stane se náhodnou obětí.

## Očekávaný vývoj a možná řešení

Zcela obdobný vývoj jako u automobilismu lze očekávat i u informačních technologií, ale s mnohem příjmemnějšími přínosy a mnohem menšími škodami. Na konferencích o bezpečnosti (naposledy v říjnu 2009 na konferenci RSA Europe) se odborníci pomalu dopracovávají k tomuto závěru: bezpečnosti lze dosáhnout jen tehdy, když je pro ni vytvořena organizační a technická infrastruktura. Není to stejné u silniční dopravy? Uvedme konkrétní příklad módního trendu využívání přenosných USB flash disků. Jejich šifrování má jistě velký smysl, avšak ještě větší bude mít v informačním systému, který byl bezpečný již před jejich příchodem. Šifrované médium je v podstatě k ničemu, jestliže ho společně s uživatelem vysává také virus nebo tzv. trojský kůň zabydlený v operačním systému. Chrise Young na konferenci RSA řekl: „Jsou tu zcela jasné přínosy

z využívání nových technologií, a abychom dosáhli lepší a efektivnější bezpečnosti, musíme ji věnovat do infrastruktury. Žádný jednotlivý produkt však neřeší ani žádný dodavatel se nechystá řešit současnou množinu problémů. Závěr je bezpodmínečný: vytvářet architekturu, která obsahuje vše, co organizace potřebuje, aby zůstala tak bezpečná, jak je to možné.“ Tedy zaprvé, bezpečnost musí řešit pouze to, co je třeba, a zadruhé, může ji vyřešit jedině v systému, v celistvosti, s podporou infrastruktury a architektury. Jednotlivá opatření nejsou účinná.

## Nové „obrcentrum“ kybernetické bezpečnosti

Jako by to slyšela americká vláda a NSA, které nedaleko Salt Lake City za 1,5 miliardy dolarů budují centrum pro kybernetickou bezpečnost. Až tato instituce, která bude v první fázi zaměstnávat jen stovky lidí, vyřeší svůj první úkol, tj. zabezpečit připojení vládních institucí k internetu, zaplatí se náklady. Každá vládní organizace totiž v současné době řeší problémy bezpečnosti a připojení k internetu po svém, a tak existuje více než 40 000 bran. Až se začne někdo centrálně starat o efektivitu připojení, bezpečnost, centrální správu a monitoring, bezpečnost i efektivita velmi rychle vzrostou. Adekvátně se zmenší ztráty, které by hackeri způsobili domácím sítím, a investice se vrátí. Kryptologie hraje v tomto procesu velmi významnou, ale neviditelnou roli. Téměř všechny bezpečnostní mechanismy ji využívají, ale v pozadí. Zejména je to autentizace uživatelů, poté autentizace zpráv, dokumentů, elektronický podpis jak dokumentů, tak zejména programů, aplikací, operačních systémů nebo jejich knihoven apod. K tomu americká vláda také vydala množství velmi užitečných norem s požadavky, jak zajišťovat identifikaci a autentizaci ve vládních sítích, jaké prostředky lze používat apod., čili vytváří infrastrukturu, bez níž by to nebyl systém, a nebylo by možné bezpečnost budovat od základu. Tyto normy mohou být užitečné i pro nás, když už je někdo zcela zdarma sepsal a dal k dispozici. Nebo to uděláme jako „Pašáci“ v našem seriálu?

Vlastimil Klíma, nezávislý kryptolog,  
v.klima@volny.cz

## LITERATURA

[1] Archivy autora a archiv článků kryptologie pro praxi. Dostupné na: <http://cryptography.hyperlink.cz>