Jaké máte heslo?

6.2.2017 Euro str. 32 Report - Kyberbezpečnost

Ondřej Stratilík

Kybernetická **obrana** je pro státy
čím dál důležitější. Zato soukromé firmy zaspaly

Temná kancelář s několika zářícími monitory a výkonnými počítači, u klávesnic mladí lidé a v pozadí **velitel** rozdávající pokyny. Nějak takhle vypadá zažitá představa hackerů útočících na počítačové sítě. Jenže realita tolik "sexy" být nemusí.

Svědčí o tom třeba příběh čtyřiadvacetiletého Brita z New Yorku pracujícího pro malou vydavatelskou společnost. Řeč je o Christopheru Gardnerovi. Mezi léty 2011 a 2012 pracoval jako webmaster ve firmě Dan's Papers. Jenže s podnikem se nerozloučil v dobrém, a tak se začal mstít.

Naboural se do FTP serveru zpravodajského webu Dan's Papers, pozměnil nastavení a výsledkem bylo, že stránky dlouhodobě vypadly z internetových vyhledávačů.
Klesla čtenost a firmě se propadly příjmy z inzerce.

Případ si vzala na starost FBI. Během vyšetřování vyšlo najevo, že Dan's Papers po odchodu Gardnera nezměnily hesla, a naštvaný útočník se tak na FTP mohl dál v klidu přihlašovat svým uživatelským jménem a kódem.

I tenhle případ dokazuje, jak jsou firmy - malé i velké - snadným terčem pro kybernetický **útok**. A že hrozbou nejsou jen sofistikované nebo státem podporované skupiny hackerů.

Kdo doplatí první?

Zatímco v **USA** se z kauzy Dan's Papers stal téměř učebnicový příklad a začalo se investovat do **obrany** před počítačovými útočníky, v **České republice** vypadá situace po dle oslovených **bezpečnostních analytiků** mnohem primitivněji. "Problémem je, že nikdo tady zatím nedoplatil na to, že něco neudělal," krčí rameny Martin Půlpán, výkonný ředitel společnosti Net.pointers.

Hřeší se na to, že **Česko** zatím není pro kybernetické útočníky příliš atraktivním cílem. "Jako ve všem jsme i v téhle oblasti trochu pozadu," varuje Půlpán před blízkou budoucností, kdy se situace obrátí a **české** společnosti nebo dceřinky zahraničních korporací se pro hackery stanou zajímavou trofejí.

“e se situace skutečně mění, potvrdilo před několika dny **ministerstvo** zahraničí. Šéf diplomacie Lubomír Zaorálek (**ČSSD**) přiznal, že hackeři z ciziny víc než rok nerušeně stahovali data z e-mai lových stránek nejvyššího vedení **Černínského paláce**. Zřejmě se dostali i k citlivým materiálům, které může někdo zneužít.

Ostatně kvůli podobným motivům divocí "ajťáci" atakují i soukromé firmy.
"Hodně záleží, co napadená společnost dělá. Kradou se informace o klientech, hackeři jdou po penězích," vypočítává Půlpán. Výjimkou podle něj nejsou ani krádeže intelektuálního know-how. Takový scénář obvykle nastává v okamžiku, kdy dvě firmy připravují fúzi a jedna z nich chce mít při vyjednávání navrch.

Bezpečnost nejde outsourcovat

Je tu ale ještě jedna důležitá okolnost, kvůli níž se bude muset soukromá sféra chtě nechtě zaměřit na kybernetickou bezpečnost. Jde o loni přijaté obecné nařízení **Evropské unie** o ochraně osobních údajů.

Firmy v členských zemích mají už jen rok a čtvrt, aby se pravidlu přizpůsobily.
Norma například zavádí povinnost informovat národní **bezpečnostní úřady** o narušení zabezpečení osobních údajů. Jinými slovy - pokud hackeři napadnou klientské databáze bank, internetových obchodů či cestovních kanceláří, firmy to musejí nejpozději do 72 hodin ohlásit.

I proto je velmi pravděpodobné, že **speciální** jednotky zaměřené na kyber **obranu** se v dohledné době stanou součástí většiny společností. Nepůjde ovšem o nic laciného. "Bezpečnost nejde outsourcovat, musíte mít vlastní lidi. Pro průměrnou firmu se jedná o dva až tři seniorní odborníky a dalších deset lidí, to znamená 15 až 20 milionů korun ročně," ví Půlpán.

Zásadní potíž představuje nedostatek expertů. Přetahují je například banky či farmaceutické firmy, aby si chránily receptury svých léků. To pociťuje i **ministerstvo obrany**, které právě buduje vlastní Národní centrum kybernetických sil pro **obranu České republiky** před **útoky** hackerů.

"Naplňování jde pomalu, o IT odborníky je velký zájem," pokyvuje hlavou Jan Beroun, ředitel **Vojenského zpravodajství**.

Univerzita obrany v **Brně** tak začala připravovat **speciální** obor, kde bude počítačové analytiky vychovávat. "Počet studentů bude předmětem dalších diskusí.

Univerzita obrany má v současné době dostatečné kapacity a potenciál k jejich zabezpečení," nechtěl zatím Vladimir Šidla, mluvčí školy, odhalit, kolik adeptů a kdy začnou učit.

Protože ale půjde s největší pravděpodobností o pětiletý magisterský obor a další pětiletku absolventi stráví nabíráním praxe, situace se nevyřeší hned.

Do té doby firmám nezbývá než skoncovat třeba s lehce odhadnutelnými a přednastavenými hesly. A aspoň občas je změnit. Ostatně lidé z Dan's Papers by mohli vyprávět.

***

Národní centrum

Novela zákona o **Vojenském zpravodajství** umožňuje vznik Národního centra kybernetických sil, jehož úkolem bude ochrana státu před nepřátelskými počítačovými **útoky**. O úpravě se vede ostrá debata, kritici se obávají, že agenti budou moct bez povolení soudu procházet třeba i obsahy e-mailů, **ministerstvo obrany** to odmítá. Nebudou pro něj prý důležitá data a obsah infi kovaných zpráv, ale především to, odkud míří. V právě budovaném centru už pracuje prvních dvacet expertů, při plném provozu se roční náklady vyšplhají na 300 milionů korun.

Foto popis| Do prvního maléru. „Problémem je, že nikdo tady zatím nedoplatil na to, že něco neudělal," krčí rameny Martin Půlpán, výkonný ředitel společnosti Net.pointers.
Foto autor| FOTO: Martin Pinkas

O autorovi| Ondřej Stratilík mailto:stratilik@mf.cz