komora.cz

SPOLEČNÍK VE SVĚTĚ PODNIKÁNÍ A PRŮMYSLU

www.komora.cz | Měsíčník Hospodářské komory České republiky | prosinec 2017 – leden 2018 | ročník 18

Muž, který věřil vinylu

Zdeněk Pelc, GZ Media

Řád Vavřínu 2017

Makroekonomická prognóza HK ČR

Téma: O čem se bude mluvit

Měsíčník Hospodářské komory České republiky | prosinec 2017 – leden 2018 | ročník 18

www.komora.cz

Na internetu není nic zadarmo

KAROL SUCHÁNEK

Informační technologie jsou pro Karola Suchánka koníčkem už od střední školy. Bezpečnostní software, který vyvinul v šestnácti letech, vyhrál středoškolskou soutěž a dostal se až do běžného prodeje. První část profesionální kariéry pracoval na vývoji softwaru a získal titul 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 tématu cybersecurity, o kterém dnes přednáší a organizuje semináře pro veřejnost. Ve firmách organizuje cybersecurity koučink pro klíčové zaměstnance a jejich rodiny. Je absolventem speciálního cybersecurity programu na Massachusetts Institute of Technology (MIT) v Bostonu.

V životě jsou tři lidé, které byste si neměli za žádnou cenu rozhněvat. Váš partner, protože riskujete tichou domácnost. Váš kuchař, protože má moc nad tím, co jíte. A váš IT, protože právě on o vás ví úplně všechno. Právě proto jsme se zeptali Karola Suchánka, specialisty na kybernetickou bezpečnost, jak účinně předcházet hrozbám, které dnes číhají na firmy v online prostoru.

Co je pro firmu největším nebezpečím?
I když si to často ani neuvědomujeme, virtuální svět je dnes velmi propojen s tím skutečným. Naše práce se snadno prolne do soukromí a naopak. Je proto důležité najít ve firmě striktní, ale zároveň komfortní politiku toho, co zaměstnanec smí a nesmí dělat na počítači. Protože největší hrozbou jsou právě samotní uživatelé.

Co tedy můžeme udělat pro to, abychom ochránili firemní data?
Na prvním místě je školení zaměstnanců. Mělo by proběhnout nějakou interaktivní formou, aby si z něj lidé opravdu něco odnesli. Další možností je testování. Existují firmy, které se na tuto činnost specializují. Rozešlou vašim zaměstnancům fishingové e-maily a pak se čeká, kdo se chytne. Podle výsledků se může například zjistit, že některý ze zaměstnanců se pravidelně pohybuje na špici pomyslného žebříčku „nachytaných" a vyjde najevo, že už dva roky nebyl na žádném školení o bezpečnosti.

Existují ještě další testovací metody?
Můžete ve firmě rozmístit flashky a opět počkat, kdo si ji vezme a připojí do počítače. Pokud obsahuje vir, máte problém. Tímto způsobem mimochodem probíhají konkurenční boje mezi společnostmi. Další praktikou je tailgating. Na recepci se vydáváte za někoho jiného a přesvědčíte recepční, aby vás odvedla k firemnímu serveru. Jste například John z Microsoftu, máte podezření, že šéf firmy krade software, a musíte to tajně prověřit. Pokud vás tam recepční opravdu odvede, je na čase, aby firma striktně stanovila postupy, kterými se mají zaměstnanci řídit.

Týká se to i IT oddělení?
IT oddělení o vás ví úplně všechno. Má všechny přístupy, ví, kdy budete propouštět nebo nabírat nové zaměstnance, protože má na starosti jejich uživatelské účty. Ale i práci IT je potřeba někdy zkontrolovat. K tomu slouží externí audit, který si můžete objednat.

Zmínili jsme rizika spojená s lidskou chybou. Jak chránit samotný server a počítače před napadením?
Určitě je dobré mít správně nastavené security ve firmě, mít bezpečnostní software. Dále zajistit, aby si zaměstnanci nemohli sami stahovat a instalovat programy. A užitečnou věcí je také zašifrovaný disk. Pokud ho zašifrovaný nemáte a já se dostanu k vašemu počítači, stačí mi fyzicky disk vyjmout, vložit do mého počítače a už jsem u vašich dat. Lidé by proto neměli nechávat počítače ležet volně na stolech. Někde jsou proto vybaveni kensingtonským kabelem, někde zamykají počítače na noc do sejfu. Nikdy totiž nevíte, kdo se v noci ve firmě k vašemu počítači může dostat. Prevence je lepší, než pak řešit případné následky.

Jak se ale vypořádat s tím, že tato opatření jdou často proti provozním požadavkům firmy?
Do IT technologie nechce vedení obvykle příliš investovat. Když investujete čtvrt milionu do online reklamy, tak hned druhý den máte výsledky. Zatímco pokud tu stejnou částku investujete do IT, nezmění se nic. Ikonky v počítači jsou stále stejné, změna není vidět. Ale ve finále vám může ušetřit obrovské výdaje. Samozřejmě není nutné kupovat IT ochranu za čtvrt milionu. Vše záleží na charakteru a velikosti firmy. Pamatujte si, že na internetu nic není zadarmo, vždy za to zaplatíte minimálně svými daty. A to je nakonec vlastně to nejcennější. ■

LUCIE SLOVÁKOVÁ