Univerzita čelí kyberútokům. Podvodné e-maily jsou věrohodné, varuje expert

Univerzita občas čelí kyberútokům. Podvodné e-maily jsou věrohodné, varuje expert

Autorka tohoto článku jednoho dne otevřela svou soukromou elektronickou schránku a ztuhla: *Rádi bychom vás informovali o nezaplacené pohledávce, kterou u vás evidujeme. Oznámení vám bude doručena ještě písemně. Zatím jsme v tomto ohledu nepodnikli žádné další kroky, ale pokud uvedenou částku nezaplatíte, budeme nuceni ji po vás vymáhat soudně. Všechny podrobnosti ohledně vašeho dluhu zasíláme v příloze…* Roztřeseným prstem udělala „klik“ a samozřejmě jediné, co v příloze našla, byl trojský kůň.

Zrádnost internetové komunikace tkví v tom, že je pro uživatele velice osobní. Většina lidí, pokud tedy zrovna nespí, je on-line. Současně roste jejich přesvědčení, že virtuální svět dobře znají a nic je v něm nemůže překvapit. To je velký omyl. Když přijde zrada, nevěří tomu, jsou zaskočeni a ve stresu pak dělají chyby. Zpětně je jasné, že šlo o podvodný e-mail. A určitě se teď naprostá většina počítačově gramotných čtenářů chytá za hlavu, jak může člověk na něco tak triviálního skočit. Ale někdy se prostě přihodí, že neznámý hacker – třeba i z druhé strany planety – se přesně trefí do citlivého místa oběti. Například jste nedávno provedli přes internetové bankovnictví hodně plateb a teď si nejste jisti, zda se všechny v pořádku odeslaly. Nebo vás chytil revizor a vy jste sice pokutu zaplatili, jenže až po delší době, a co když je tam nějaké penále z prodlení? <blockquote class="leftfloat"> Útoky hackerů bývají psané dobrou češtinou a velmi přesně zacíleny. Pokud máte tu smůlu, že se vás emočně dotknou, můžete přijít i o peníze </blockquote>

Cílený útok na konkrétního zaměstnance

Podle Vladimíra Horáka z Ústavu výpočetní techniky Univerzity Karlovy jde o typickou reakci. „Naprostá většina lidí, kterým se takový útok stane poprvé, zareaguje podobně. Strach jim nedovolí tu přílohu smazat. Až se vám to stane příště, budete už poučená.“ Ano, nejspíš. Jenže toto byl pouze jeden vzorový případ. Typů hackerských útoků je mnohem víc, jsou stále rafinovanější, leckdy bývají psány dobrou češtinou a nezřídka jsou i velmi přesně zacíleny. Opět platí – pokud mají oni to štěstí a vy tu smůlu, že vás emočně zasáhnou, můžete kromě zavirování počítače přijít i o peníze. „Buďto rozešlou několika tisícům lidí stejný e-mail typu: *Gratulujeme, vyhráli jste milion korun. Abychom vám je mohli poslat, potřebujeme znát číslo vašeho bankovního účtu, kreditní karty a PIN.* A čekají, kdo se chytne,“ vysvětluje Vladimír Horák a přidává druhou možnost – cílený útok: „V případě univerzity si například zjistí jméno šéfa a jeho podřízeného, nejlépe účetního. Tomu pak napíšou e-mail, který zdánlivě vypadá, jako by ho odeslal vedoucí: *Potřebujeme rychle odeslat xxx euro na zahraniční účet. Můžeš to zařídit?* Pokud je nadřízený naneštěstí zrovna delší dobu mimo kancelář či dokonce v zahraničí, vypadá najednou takový pokyn velice věrohodně. A co teprve ve chvíli, kdy na nějaký upřesňující dotaz dokáže hacker odpovědět.“ Nejde o žádný scifi scénář, s takovýmito útoky se univerzita opravdu čas od času potýká. Peníze zcizeny nikdy nebyly i díky zavedeným pravidlům pro práci s fakturami, kdy jejich proplacení nemůže odsouhlasit pouze jeden člověk. Nicméně stalo se, že si zaměstnanec na základě takové zprávy připravil podklady k zaplacení a čekal, až se vedoucí vrátí a projednají to spolu osobně. Když pak zjistí, že šlo o podvod, jsou z toho oba velice překvapení a vyděšení.

<blockquote class="rightfloat"> Nejrizikovější je pondělí. O víkendu většina lidí emailovou schránku neotvírá, a počítačoví experti se tak o problému nedozví </blockquote>

Obezřetnost se vždy vyplatí

Lidé totiž mají internetové podvodníky zafixované jako pisatele podivných špatně čitelných zpráv, které obvykle končí ve spamu. „Opravdu dokážeme díky počítačovým filtrům a antivirovým programům většinu věcí zachytit. Ale jsme stále v závěsu – můžeme pouze reagovat na to, co hackeři vymyslí. Proto potřebujeme informace od uživatelů, že jim do pošty přišlo něco podezřelého, abychom to mohli řešit co nejrychleji,“ říká Vladimír Horák s tím, že nejrizikovější je v tomto ohledu pondělí. Během pracovního týdne dokážou lidé z IT vyřešit internetové hrozby v řádu hodin jenom díky tomu, že se jim ozve obezřetný zaměstnanec. Jenže o víkendu spousta lidí e-mailovou schránku neotvírá, a počítačoví experti

se tak o riziku nedozvědí. V pondělí ráno už mají „nakaženou“ zprávu v elektronické poště všichni a pravděpodobnost třeba i jen jediného „odkliknutí“ roste.

Nebojte se požádat o pomoc

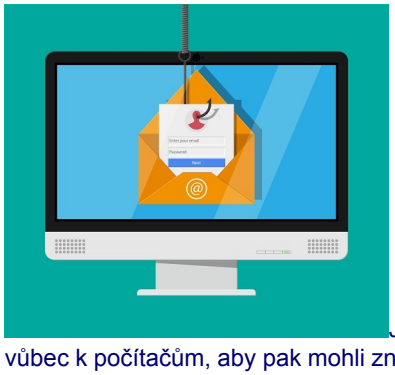
„Proto bych chtěl apelovat na zaměstnance a studenty, aby se neostýchali a při jakýchkoli pochybnostech nás kontaktovali. Je to pro nás důležitá zpětná vazba jak se dozvědět o nějaké nové vlně podvodů. A stejně tak pokud se už někdo obětí internetového útoku stal, ať se nebojí to oznámit. Čím dřív problém začneme řešit, tím menší dopad to na něho potažmo celou univerzitu bude mít. Lidé dělají chyby, to je úplně normální,“ uzavírá Vladimír Horák.

Na co si dát pozor

GDPR a přeposílání pracovních e-mailů na soukromé adresy

Univerzita Karlova stejně jako všechny organizace v Evropské unii podléhá GDPR a musí dodržovat určitá pravidla pro ochranu osobních údajů lidí, kteří s ní přichází do styku. Z titulu své činnosti může shromažďovat údaje pouze od svých zaměstnanců a studentů. Ve všech ostatních případech musí dotyčnému vysvětlit, k čemu jeho osobní údaje potřebuje a získat k tomu jeho souhlas. Pokud si zaměstnanec univerzity přepošle korespondenci z pracovního e-mailu na soukromý, je to něco, s čím nedal druhý pisatel souhlas. Univerzita je povinna jeho údaje zabezpečit proti zneužití, což po přeposlání na cizí e-mail nedokáže zajistit. A jde tudíž o porušení GDPR.

Phishing



Jde o útoky, kdy se podvodníci snaží získat přihlašovací údaje k e-mailům nebo vůbec k počítačům, aby pak mohli zneužít například servery či adresáře instituce. V praxi to funguje tak, že rozešlou e-mailové zprávy, které vyzývají adresáta k zadání osobních údajů na falešnou stránku, jejíž podoba je takřka identická s tou oficiální. Stránka může například napodobovat přihlašovací okno internetového bankovnictví. Uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze.

Při sebemenší pochybnosti si pravost e-mailu a pokynů v něm uvedených ověřte u pracoviště podpory nebo u správce sítě. Pokud jste omylem „podlehli“, oznamte to tamtéž a co nejdříve si změňte heslo. Můžete se také obrátit na bezpečnostní tým počítačové sítě Univerzity Karlovy CSIRT-CUNI , který je provozován Ústavem výpočetní techniky UK.