Hackeři se do Sobotkova účtu možná vůbec nedostali

ZPŮSOB, JAKÝM HACKEŘI ZVEŘEJNILI E-MAILOVOU KOMUNIKACI ČESKÉHO PREMIÉRA, NASVĚDČUJE TOMU, ŽE JEHO ÚČET NEMUSELI PROLOMIT. MOŽNÁ SE ALE VLOUPALI DO SOBOTKOVA POČÍTAČE NEBO MOBILU.

Tomáš Pojar
prorektor vysoké školy CEVRO Institut, bývalý velvyslanec v Izraeli

Tomáš Rosa
přední český expert na aplikovanou kryptologii

Pavel Růžička
odborník na bezpečnost IT, občanský spolek Brmlab

Michal Špaček
vývojář webových aplikací, lektor

Tomáš Pergler
redaktor Týdeníku Echo

Napadení a zveřejnění e-mailové komunikace premiéra Bohuslava Sobotky je pravděpodobně dosud nejvážnějším kybernetickým útokem do nejvyšších míst české politiky – tedy z těch útoků, které vypluly na povrch. Dostali se nacionalističtí hackeři do Sobotkova soukromého e-mailu přes prolomení jeho hesla, nebo je pravděpodobnější jiná cesta? A stojí za útokem opravdu hackeři, kteří nesnášejí uprchlíky? Jakou zkušenost si máme z tohoto případu odnést? Do Salonu Týdeníku Echo přišli diskutovat jeden z nejuznávanějších českých odborníků na kryptologii Tomáš Rosa, Pavel Růžička z pražského hackerského spolku Brmlab, bezpečnostní analytik a diplomat Tomáš Pojar a odborník na internetovou bezpečnost Michal Špaček.

Co můžeme o případu Sobotkova e-mailu vyvodit z informací, které se zatím dostaly na veřejnost?

Rosa: Víme, že někdo ukazuje fotky obrazovek, na kterých jsou vidět maily a texty premiéra. K těmto datům se dalo dostat mnoha způsoby. Nutně nemuselo dojít k prolomení účtu e-mailového serveru, jakkoli se to velmi nabízí. Mohl to být škodlivý kód v počítači, napadení připojení počítače přes nejbližší Wi-Fi síť... možností je spousta. Ta skutečnost, že nevíme, co se vlastně stalo, znamená, že sami nevíme, do jaké míry tomu mohl premiér nebo někdo jiný zabránit.

Špaček: Mně přijde poměrně zajímavý způsob, jakým se ta data zveřejňují. Nikdy předtím jsem neviděl, že by někdo zveřejňoval uniklou korespondenci přes screenshotování (snímkování). Navíc tam nejsou jenom Sobotkovy e-maily, ale i jiných lidí a všechny jsou nafocené stejně. Ještě bych připomněl případ premiérova účtu na Twitteru, který byl evidentně napaden.

Rosa: Jde o to, jak se k tomu účtu dostali. Když ovládnete počítač, tu cestu máte poměrně přímočarou. Osobně, pokud bych byl v roli, že mám někomu prolomit přístup do mailu, na Twitter nebo na Facebook, sázel bych nejdřív na štěstí, že ten člověk bude mít všude stejné heslo. Bude-li svědomitější a hesla budou různá, určitě bych

Diskutující v Salonu Týdeníku Echo: zleva Michal Špaček, Tomáš Rosa, Tomáš Pergler, Tomáš Pojar a Pavel Růžička
Foto: Jan Zatorsky

se zaměřil na jeho počítač, na mobil, kde se to všechno schází v jednom.

Pojar: Já jsem se na ty screenshoty nedíval. Ale chci poznamenat, že na Twitteru píší za premiéra příspěvky jiní, takže to rozšiřuje počet lidí, kdo má přístup k jakým heslům. Nebo koneckonců stačí do zařízení strčit USB, a máte ho infikované.

Rosa: Těžko suplovat to, co už nyní vědí orgány činné v trestním řízení. Předpokládám, že Seznam jim sdělí nějaké podrobnosti, jako kdy bylo na tu stránku přistupováno, z jakých adres. To už napoví mnoho. Pokud uvidíte, že se tam přistupuje jenom z adres, které jsou obvyklé, a najdete je tam dva roky zpět, signalizuje to infekci počítače. Pokud bude jasně vidět, že je tam přístup z úplně různých adres a zrovna v korelaci s tím by došlo k nějakým útokům, dá se z toho vyvodit, že by někdo disponoval heslem. Ale těch možností a variant je opravdu mnoho.

Pojar: Lidé, kteří pracují v bezpečnostních firmách a službách, říkají, že nejméně na 90 procent je tam nakonec, když se chtějí někam dostat, klíčový lidský faktor. Ať už je selhání vědomé, nebo nevědomé. Jsem přesvědčený o tom, že v této kauze, ať už to byl premiér, nebo někdo další, je lidský faktor naprosto zásadní.

Ta webová stránka je údajně hodně amatérsky udělaná. Je skutečně primitivní?

Růžička: Ta stránka je strašná.

Špaček: Každý není webový designér, navíc u takového tématu. Zveřejněné úniky dat, které jsem zatím viděl, byly celé texty, třeba i vytažené z e-mailu. Ale screenshotované e-maily, to mi přijde minimálně divné.

Rosa: Je důležité poznamenat, že základní službou, kterou poskytuje škodlivý kód, když se uhnízdí v počítači oběti, je posílání videí a screenshotů z jejich obrazovek.

Pojar: Existují studie, podle nichž se ve světě na každých deset milionů dolarů do hardwaru a softwaru investuje jen osm dolarů na lidi.

Tato forma je nezvyklá pro prezentaci ukradených e-mailů, používá se více méně jako důkaz toho, že jste v zařízení. Útočník se tedy mohl dostat k datům touto cestou. To je na jednu stranu plus, protože e-mailová schránka není tolik napadená. Na druhou stranu je tu i minus, protože útočník působí v potenciálně ještě citlivějším prostředí, v operačním systému počítače premiéra. Samozřejmě záleží na tom, co je to za počítač, jak k němu premiér přistupoval. Základem všeho je, že taková data v soukromé e-mailové schránce neměla být.

Špaček: Kdybych se někomu vloupal do schránky, snímkovat jednotlivé maily je fakt strašná práce. To je lepší stáhnout celý balík a jít co nejrychleji pryč, abych zanechal co nejméně stop. Když to snímkuji, už dávám nějakou informaci – například podle fontu poznám operační systém. Když data vezmu z e-mailové schránky nebo ze serveru v původním zobrazení, nenechávám za sebou žádný potenciální identifikační znak.

Pojar: Stránka, kde to bylo zveřejněno, je usídlená někde v Kalifornii. Já jenom doufám, že relevantní české bezpečnostní složky už do té stránky dávno pronikly. Jestliže ne, máme tady velký problém se z toho stavu někam dostat. A je to na hluboké zamyšlení, jaké schopnosti máme.

Rosa: Pokud příslušné složky našeho státu nejsou schopny proniknout do toho serveru, mohou si to odněkud objednat – vzpomeňme si na loňský případ firmy Hacking Team. Jsou tady desítky firem, které si najímají například banky. Tyto firmy jsou připraveny se do takového serveru s vysokou pravděpodobností dostat během 24 hodin. Přinesou vám na stříbrném podnose všechno, co tam je.

Pojar: A někdy si je najímají i státy.

Rosa: Na druhou stranu si může druhá strana najmout na černém trhu firmu, která provede útok za ni. Pak je to souboj kapitálu. Je tedy otázka, zda jsou za těmi stránkami jenom hackeři, nebo nějaký kapitál.

Špaček: Nemyslím si, že by tahle skupina útočníků byla nějak obzvlášť na výši. Všechno mě navádí k tomu, že to jsou ne úplně technicky zdatní lidé.

Růžička: Minimálně to sedí podle toho, co prezentují. Může to ale být také maskovací manévr.

Pojar: Existuje určitá regulace některých z těch sofistikovaných hackerských firem ze strany státu. Není možné si některé z těch špičkových firem ve světě najmout na komerční bázi. Pokud jsou státy dostatečně kreativní, mají trochu navrch. V Rusku nebo v Číně je to trochu něco jiného, ale i tam jsou tyto firmy pod významnou kontrolou státu. Když si pak někdo najme takovou ruskou nebo čínskou firmu čistě na komerční bázi, můžete si být jisti, že ten čínský nebo ruský stát o tomhle věděl.

Dbá se v Česku dostatečně na kybernetickou bezpečnost? Myslím z pohledu státu i jednotlivců.

Pojar: Je otázka, jak se veřejnost nebo jednotliví aktéři cítí ohroženi. To ohrožení bývá pociťováno ve chvíli, kdy se už něco stane. Jestli je Sobotkova kauza k něčemu dobrá, pak k tomu, že jsme si uvědomili, že nejvyšší lidi ve státě se snaží někdo nabourat, že to doopravdy hrozí. Jsem hluboce přesvědčen, že elektrické přenosové sítě budou lépe chráněny, až některá z nich padne. Jen doufejme, že to nebude v Česku. Dokud se to děje na druhém konci světa, nikdo si to moc neuvědomuje. Když se loni nebo předloni utavila po hackerském útoku vysoká pec v Německu, nějakým způsobem to rezonovalo i tady.

Špaček: Spousta uživatelů nevidí hodnotu své e-mailové schránky nebo svého počítače. Na svých přednáškách se často setkávám s tím, že až když lidem ukážu naživo, jak jednoduše se dají některé věci podniknout, zpozorní a připustí si, že se něco takového může stát i jim.

Růžička: Byla doba, kdy se na bezpečnost moc nehledělo. Teď se to zlepšuje. Rozšiřují se i možnosti šifrované komunikace. Na co by se měli vývojáři softwaru soustředit, je použitelnost pro běžné lidi.

Používáte e-mailové účty u českých portálů?

Růžička: Mám tam účet, ale nepoužívám ho. Když už bych ho používal, pak s nějakým šifrováním. Ono je také šifrování a šifrování. Někdy šifrujete jenom komunikaci mezi vámi a poskytovatelem, tedy například Seznamem, a někdy můžete šifrovat od odesilatele k příjemci, což je pravděpodobně i pro takové ty třípísmenkové agentury dodneška problém rozšifrovat.

Rosa: Já používám účty mnoha druhů, mezi nimi i na těchto veřejných serverech. Musím říct, že velmi pečlivě vážím, co takovému účtu svěřím. Beru to tak, že kdyby se někdo k těm zprávám dostal, nevznikne mi z toho žádná újma. Snažím se případnému útočníkovi ztížit situaci, jak se dá. Ale jestli mu to přesto stojí za to a chce vědět, jaké přezdívky používáme v partě kamarádů, už s tím nic nenadělám.

Bylo by řešením zakázat veřejně činným osobám používat soukromé e-maily? Bylo by něco takového vůbec reálné?

Špaček: Určitě se to zakázat dá, ale oni si určitě najdou cestičku, jak to obejít. Pokud někomu nebude uživatelsky vyhovovat státní e-mail, prostě si udělá účet na Seznamu či jinde. V jedné firmě, kde jsem pracoval, bylo zakázáno používat externí e-mailové servery, z pochopitelných důvodů, například kvůli ztrátě zdrojových kódů. Stejně si tam někteří lidé nastavovali přesměrování. Zakázat se to dá, ale pokud se to nedá systémově vynutit, stejně se to bude obcházet.

Rosa: Podívejme se na to realisticky. Když si koupíte zařízení s operačním systémem Android, ve většině jeho klonů se v podstatě předpokládá, že budete mít účet na portálu Google. Už jenom proto, abyste si mohl stahovat aplikace. Jakmile máte účet na Google Play, máte tím pádem automaticky nějakou e-mailovou adresu. Tu vám systém zkrátka přiřadí, ať se vám to líbí, nebo ne, a bude ji používat. Po čase vás to zlomí a vy si řeknete, když už tu adresu mám, budu ji používat. Když si vezmeme konkurenční Apple, a priori nemá podmínku založení účtu a e-mailu, ale tak nějak se předpokládá, že vaše Apple ID bude ve formě e-mailové adresy. Na ni vám postupně začnou chodit faktury za iTunes a tak dále.

Pane Pojare, vy máte zkušenost z diplomatického působení v Izraeli. Je tam viditelný rozdíl v zabezpečení komunikace ve státní správě oproti nám? Je myslitelné, že by se tam přihodilo něco takového jako českému premiérovi?

Pojar: Myslitelné to nepochybně je, na druhou stranu ta pravděpodobnost je asi menší než jinde, protože Izraelci neskutečně investují nejen do technologií, ale také do svých lidí. A jsme zase u toho. Existují studie, podle nichž se ve světě na každých deset milionů dolarů do hardwaru a softwaru investuje jenom osm dolarů na lidi. Toto samozřejmě v Izraeli funguje jinak, protože ta země je ve válce, také v kybernetické válce, je neustále napadána. Povědomí a systémy jsou tam na úplně jiné úrovni. Mimochodem, já vůbec nevím, jestli izraelský premiér má e-mail. Nebyl bych překvapený, kdyby žádný neměl. Jistě nějaký existuje, ale s ním operují jiní lidé určení pro komunikaci. Ano, nejsme v situaci, kdy bychom se měli chovat jako Izraelci, aspoň zatím. A ani neviním českého premiéra za to, že používá e-mail a má více adres, mně to přijde zcela normální. Otázkou je, co se do těch e-mailů píše a kde je nějaká hranice, kdy můžu být vydíratelný.

Rosa: Ono to souvisí s něčím, co se vznosně nazývá počítačová gramotnost. Já z ní mám spíš takovou pachuť. Obecně se očekává, že inteligentní člověk pohovoří o umění, posledních trendech v právu, je schopen provést základní diagnostiku onemocnění... trochu přeháním, ale všichni se snaží v těchto směrech orientovat. Ovšem pokud jde o počítačovou gramotnost a technické záležitosti, je vydáváno za intelektuální přednost veřejně a nahlas prohlašovat, že těmhle věcem vůbec nerozumím. Čím méně o nich vím, tím jsem jakoby inteligentnější. Společnost je velmi humanitně zaměřená. Neříkám, že je to špatně, ale ona je jenom humanitně založená. Jestliže jsme nad všechno takto povzneseni a technika se nás netýká, pak se o ty vidle občas bodneme.

Růžička: Možná by bylo dobré, kdybychom stejně jako na pravidelné prohlídky k lékaři chodili také ke svému expertovi přes počítačovou bezpečnost. Ten by nám dával doporučení, případně vymazal škodlivý kód.

Pomohla by nějaká centrální autorita, která by šířila vzdělání v informačních technologiích? Například samostatné ministerstvo informací?

Rosa: Už se to děje přes ministerstvo školství. Podle mě od stejného okamžiku, kdy jsou děti konfrontovány s tím, že existuje výtvarná výchova, hudební výchova, čeština a matematika, by měly vědět i to, že existuje informatika. Na základních školách už to je, i když to vypadá spíš jako kurz ve stylu Nebojte se počítače, ale to se časem poddá.

Pojar: Jednu takovou instituci tady máme, je to Národní bezpečnostní úřad. Vždycky se ho zastávám a zároveň vysvětluji, proč to spadá pod NBÚ. Tuto agendu nechtělo mít na starosti žádné ministerstvo. Samozřejmě to není velká instituce s velkým rozpočtem, ale nějakým způsobem se to v Česku rozmotává. Ve srovnání s mnoha zeměmi v Evropě, a to se nemusíme dívat jenom do střední Evropy, je tady aspoň nějaká snaha.

Rosa: Vezměme to analogicky. Máme tady institut hlavního hygienika. Nakolik nám pomáhá v prevenci rýmy? Nakolik ho potřebujete na řešení běžných zdravotních potíží? Prakticky vůbec. Asi stejně užitečná by v tomhle směru byla autorita pro bezpečnost.

Máme také Národní centrum kybernetické bezpečnosti, které funguje jako součást NBÚ.

Špaček: Pro něj ale platí to, o čem mluvil kolega. Pro spoustu malých uživatelů a firem je toto centrum k ničemu. Stejně jako zákon o kybernetické bezpečnosti. Spíš než mít nějakou centrální autoritu, zákony a ústavy je třeba říkat, že bezpečnost je každého zodpovědnost.

Pojar: Ano, ale hlavním cílem kybernetického centra není šíření obecné gramotnosti, nýbrž ochrana kritické infrastruktury.

Růžička: Co vím, seznam kritických infrastruktur vznikal na základě dotazníků, do nichž si úřady napsaly, co považují za důležité. Takže takový seznam by ještě určitě měli revidovat odborníci, kteří jsou schopni zanalyzovat, kde jsou jaká data uložena a jaká je jejich povaha. ■

Rosa: Pokud jde o počítačovou gramotnost, je vydáváno za intelektuální přednost veřejně a nahlas prohlašovat, že těmhle věcem nerozumím.