Data stran? Lákadlo pro hackery

Stranické servery jsou před volbami plné cenných dat o členech a sympatizantech. To vše mohou útočníci ukrást a zneužít

BLAHOSLAV HRUŠKA

ILUSTRACE RICHARD CORTÉS

PRAHA Datová úložiště, která používají politické strany, jsou za normálních okolností pro hackery nezajímavým cílem. Ne tak před volbami. Kromě interních stranických materiálů, z nichž by bylo možné vyčíst volební strategii, se stranické servery plní cennými daty o členech, příznivcích či sympatizantech.

Lze z nich zjistit nejen e-mailové adresy, ale i chování stranických souputníků na sociálních sítích. Pomocí služeb, které se specializují na vytěžování dat, mají strany přehled o tom, kdo, kdy a kde čte jejich příspěvky a s kým je sdílí. Snaha vědět o potenciálních voličích co nejvíce a cíleně pracovat s informacemi o jejich chování ve světě internetu jde napříč politickými stranami. Jediní komunisté přiznávají, že je sledování příznivců přes web nezajímá.

„Data o chování svých příznivců samozřejmě sbíráme, jinak bychom nevěděli nic," říká Marek Prchal, ředitel divize nových médií hnutí ANO. Podobně mluví i Jakub Hnát, mluvčí TOP 09. „Snažíme se využívat všech dostupných možností, které sociální sítě nabízejí," potvrzuje.

Pokud uživatel souhlasí s dalším zpracováním informací, jež o sobě poskytne, je taková praxe legální. Nikoliv však úplně bezpečná. Zvláště před volbami se stranické servery mohou kromě klasického napadení systému stát obětí takzvaného sociálního hackingu – útočníci mohou ukrást digitální profily příznivců některé politické strany a zneužít je k šíření pomluv a cílené propagandy.

„V politice dnešních dnů se nebojuje jen pomocí novinových rozhovorů nebo předvolebních akcí na ulicích, ale i tím, že někoho cíleně poškodíte v digitálním světě. Toto riziko je globální a netýká se jen USA," varuje Jason Mical, viceprezident firmy Fidelis Cybersecurity, který se podílel na vyšetřování „nabouraného" soukromého e-mailu Hillary Clintonové.

Strany mimo kyberzákon

Že by politické strany zvláště před volbami měly být v pohotovosti, zdůrazňuje i Radek Holý, expert Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). „Vzhledem k tomu, že ve světě i v Evropě došlo během voleb k některým kyberútokům s různou úspěšností, nelze toto riziko v žádném případě podceňovat," říká s dodatkem, že nemá informace o konkrétních hrozbách.

Jestli by strany dokázaly na případný útok správně reagovat, sám posoudit nedokáže. „IT systémy politických stran nespadají pod zákon o kybernetické bezpečnosti, takže nemáme k dispozici potřebné informace," doplňuje Holý.

Jisté je, že se žádná politická strana na NÚKIB, který od léta bdí nad bezpečným internetem ve státní správě, zatím neobrátila.

Strany se spoléhají na své vlastní IT experty. Přístupy se ale velmi liší. LN oslovily jednotlivé strany, které by podle posledních průzkumů překročily pětiprocentní hranici pro vstup do sněmovny, a vyžádaly si informace o tom, zda před volbami věnují digitální komunikaci zvýšenou ochranu.

Z miniprůzkumu vyplývá, že zřejmě nejdál v ochraně dat jsou Piráti. Tedy paradoxně strana, která svůj program postavila mimo jiné na liberálním přístupu k digitálnímu světu. O jejich vlastní pokladnici stranických dat to neplatí.

„Zavedli jsme vyšší izolaci systémů, udělali jsme audit oprávnění, ověřili jsme obnovení ze zálohy," vypočítává přípravu na volební kampaň Karolína Sadílková, mluvčí Pirátů. Ti jsou mimochodem jednou z mála stran, které nejenže provozují vlastní server, ale samy si ho také spravují. Na rozdíl třeba od komunistů, kteří využívají cloudové úložiště, nebo Zelených, kteří svá data rovnou „zaparkovali" v sousedním Německu.

Posílení ochrany před volbami hlásí třeba také Starostové a nezávislí, jejichž někteří členové přešli při logování na stranické servery na dvoufázové ověřování. Kromě hesla tak zadávají například vygenerovaný kód zaslaný formou SMS.

Politici raději mlčí

Dělat obecné závěry, jak by strany zvládly případný útok na cenná data, která o svých sympatizantech shromažďují, nelze. Hned tři strany – ČSSD, ODS a lidovci – totiž odmítly cokoliv konkretizovat. Právě s odvoláním na bezpečnostní postupy. „Zabezpečení průběžně vyhodnocujeme a aktualizujeme, tak aby riziko nabourání bylo minimalizováno," napsal mluvčí Lidového domu Mikuláš Klang.

VOLBY 2017
zbývá 16 dní

Právě ČSSD se přitom v minulosti stala cílem útoku hackerů, kteří pustili do světa citlivé informace ze stranické kuchyně. Koncem roku 2015 se skupina napojená na rasistický web White Media nabourala do soukromého e-mailu premiéra Bohuslava Sobotky a zveřejnila mimo jiné jeho korespondenci se stratégem ČSSD Otou Novotným.

Letos v lednu pak vyšlo najevo, že se neznámí hackeři několik měsíců pohybovali také na serveru ministerstva zahraničí, které vede volební lídr sociálních demokratů Lubomír Zaorálek.

Minimálně jedno ponaučení si z toho ČSSD odnesla. Na rozdíl od loňských voleb, kdy byly soukromé e-maily špiček sociální demokracie veřejně dohledatelné na webu, politici ČSSD dnes zveřejňují jen svou oficiální e-mailovou stranickou adresu.

Soukromý e-mail do politiky nepatří

V předvolebním boji se hraje i o to, jak poškodit soupeře na webu, říká **Jason Mical**, viceprezident Fidelis Cybersecurity.

BLAHOSLAV HRUŠKA

LN Hackerské útoky se před volbami vyskytly ve Francii a USA. V Česku máme 16 dní do voleb. Myslíte, že bychom se měli obávat?

Obecně je má zkušenost taková, že štáby politických stran příliš nedbají na kyberbezpečnost. Přitom se u nich zvlášť před volbami sbíhají citlivá data o členech a sympatizantech. Vysoké nebezpečí panuje v systémech, kde se voliči nejprve musí registrovat. Tedy třeba právě v USA.

LN Takže v Evropě máme to štěstí, že můžeme jít přímo do volební místnosti?

Jiná rizika ale zůstávají. Kromě politických stran, které s daty nakládají, tu je vždy cesta od odevzdaného hlasu, který se musí zpracovat a elektronicky poslat někam do ústředí. Architekturu a ochranu takového systému je třeba pečlivě ohlídat.

LN U útoků na bankovní účty je motiv jasný – vydělat peníze. O co jde lidem, kteří se snaží nabourat do e-mailů politiků?

Tak například soukromé e-maily Hillary Clintonové obsahovaly i citlivé informace. Jistě víte, že řada z nich pronikla na různé platformy, jako třeba WikiLeaks. Důvod byl jednoduchý – ona měla vypadat jako ta špatná, zatímco Donald Trump jako důvěryhodnější kandidát. Záměrem bylo poškodit její reputaci, přesvědčit voliče, aby ji nevolili.

Ten kapitál tedy nebyl finanční, ale politický. V politice dnešních dnů se nebojuje jen pomocí novinových rozhovorů nebo předvolebních akcí na ulicích, ale i tím, že někoho cíleně poškodíte v digitálním světě. Toto riziko je globální a netýká se jen USA.

LN Spekulovalo se, že za útokem na e-maily Clintonové stojí Rusko. To se prokázalo?

Stoprocentní důkazy, které by obstály například u soudu, v ruce nemáme. Ale máme přehled o ruských aktivitách v jiných regionech a ze stop, které jsme měli k dispozici a analyzovali, vyplývá, že k útoku byla mimo jiné použita ruská klávesnice. Není to neprůstřelné, ale důkazů existuje více.

LN Soukromé e-maily používá i řada českých politiků.

Poradil bych jim jednoduché pravidlo – pokud nechcete, aby něco proniklo na veřejnost, nepoužívejte veřejně dostupné služby. Citlivé informace patří do vládních nebo stranických e-mailů, které jsou postavené na nějaké bezpečnostní architektuře.

LN Jenže používání soukromého e-mailu je i pro politiky jednodušší. Bez problému ho třeba spárujete se svým mobilním telefonem.

Jistě, jednoduché ovládání a vysoká bezpečnost většinou nejdou dohromady. Uživatelský komfort chápu. Pak ale pro politiky platí stejná pravidla jako pro kohokoliv jiného. Alespoň bezhlavě neodpovídejte na nedůvěryhodné e-maily. Lidé si často říkají, že zrovna o jejich e-mail určitě nikdo mít zájem nebude. To je ale hloupost. Objednáváte v e-shopu? Máte v e-mailu kontakty? Pak jste potenciálním objektem zájmu. Každý žijeme v ohrožení.

LN Zájem hackerů o USA je obrovský. Existuje něco specifického v regionu střední Evropy, na co by se hackeři mohli zaměřit?

Žijeme v globální době, takže jestli je v ohrožení Amerika, je v ohrožení i Česko. Samozřejmě že různé vlády i firmy spravují různá data. Také typy útoků mohou být různé, od „nabourání se" do počítačových systémů až po tzv. denial of service (*DoS – cílené přehlcení serveru požadavky – pozn. red.).*

FOTO MAFRA – DAN MATERNA

Potíž je v tom, že nikdy nemůžete vědět, odkud a od koho útok vzejde. Může to být teenager, který si chce něco dokázat a nejde mu o peníze. Pak jsou ale organizované hackerské skupiny, které působí globálně a na objednávku.

LN Neustále se opakuje, že je třeba používat antivirový program a aktualizovat operační systém. Nedávno přitom vystrašil celý svět vyděračský vir WannaCry. Jak si to vysvětlujete?

Na světě jsou tisíce firem, které se zabývají kyberbezpečností a budou vám tvrdit, že právě jejich produkt je o krok napřed. Ve skutečnosti jsme ale proti hackerům všichni o krok pozadu a jen se je snažíme dostihnout. To oni jsou ve vedení. My ale dokážeme pružně reagovat.

Záleží především na vás jako na uživateli, abyste všechny bezpečnostní prvky aktualizoval. Pokud to dělat nebudete, není otázka, jestli nějaký útok přijde, ale kdy se tak stane.

Aktualizace se sice stahují samy, ale my žijeme v době, kdy chceme mít vše na jediné kliknutí. Dostat se do své pošty, objednat si zboží. Provozovatelé takových služeb – a teď mluvím i o službách pro voliče – často volí jednoduchá řešení, protože lidé chtějí mít vše dosažitelné.

LN Nebylo by jednodušší vrátit se k papíru?

Ve volbách možná ano. Ono ale nejde jen o vhození lístku v obálce. Chceme mít také rychlé a dostupné výsledky. K papíru už se nevrátíme, protože to není pohodlné a svět už takto nefunguje.

Dnes je všechno ovladatelné přes telefon. A to ani nemluvím o internetu věcí, vynálezech, jako je online lednice, nebo moderních trendech v automobilismu. Představte si, že vám někdo na dálku aktivuje ruční brzdu, pustí vám do reproduktorů svou oblíbenou hudbu a stáhne okénka.

LN Takže naše auto nás jednou dostane?

Sobecky řečeno je taková hrozba nový byznys pro naši firmu. To ale neberte doslova, protože já jsem něco jako placený paranoik.