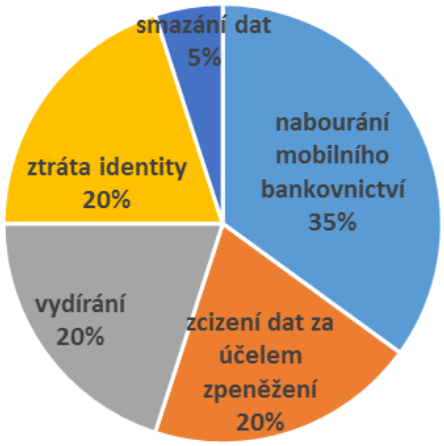
Zcizení mobilu nebo tabletu může přijít dráž než vykradení bytu

Téměř polovina populace vlastní chytrý mobilní telefon nebo tablet. Valná většina z nich přitom neodolá ani jednoduchým útokům zločinných hackerů. Neopatrným uživatelům hrozí vytunelování peněz, vydírání, zcizení identity či zablokování přístupu k osobním datům na Facebooku či Twitteru.

PRAHA, 11. srpna 2014 – Bezpečnost tuzemských domácností i firem začíná ohrožovat nový fenomén: **nezabezpečené tablety a chytré mobilní telefony**. Zatímco stolní počítače a notebooky disponují alespoň základní ochranou, v případě chytrých telefonů a mobilů tomu je naopak: „**Mobilní zařízení obvykle neobsahují ani elementární ochranu** před viry a zákeřným škodlivým softwarem – tzv. malwarem. Data uživatelé obvykle nešifrují ani nechrání silnými hesly, pravidelné zálohování je výjimkou. Přitom mobilní zařízení jsou využívána častěji než počítač," varuje **Jiří Palyza**, ředitel **Národního centra bezpečnějšího internetu (NCBI)**.

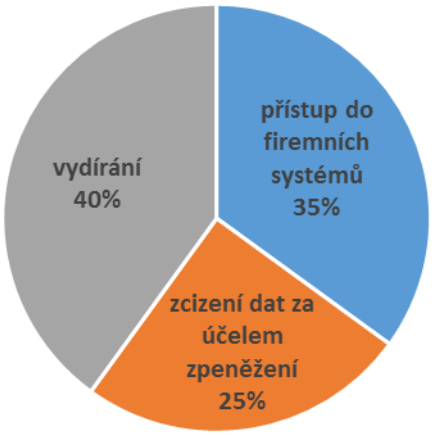
V případě útoku zákeřného škodlivého softwaru či zcizení mobilního zařízení hrozí i **běžným domácím uživatelům vysoké škody**: „Hodnota digitálních dat může snadno **převýšit hodnotu zcizitelného vybavení bytu**. Vytunelování bankovního účtu, vydírání choulostivými fotografiemi či zablokování přístupu k osobním účtům na Facebooku či Twitteru může řádově vyjít na desítky i stovky tisíc korun. Přitom šance na chycení digitálního zloděje je mizivá," varuje **Ivan Janoušek**, soudní znalec v oblasti informačních technologií ze znaleckého ústavu APOGEO Esteem.

DOMÁCNOSTI: Hrozby útoků na mobilní zařízení
(procenta vyjadřuje míru pravděpodobnosti)
Zdroj: Apogeo Esteem



Lidé totiž na mobilních zařízeních **uchovávají mnohdy více osobních dat než v osobním počítači**. „Veškeré kontakty, soukromá i firemní data, hesla, fotografie, přístup k bankovnictví, privátní i soukromá korespondence. Navíc pomocí těchto přístrojů řada uživatelů přistupuje i do firemních systémů a databází. Například pracovní e-mail má v chytrém mobilu téměř každý zaměstnanec," upozorňuje soudní znalec Ivan Janoušek.

FIRMY: Hrozby útoků na firemní mobilní zařízení
(procenta vyjadřuje míru pravděpodobnosti)
Zdroj: Apogeo Esteem



Podle zjištění APOGEO Esteem přitom mobilní zařízení používané **ve firmě dostatečně chrání jen 5–10 %** společností. V případě domácích uživatelů je situace obdobná: „Zhruba 10 % uživatelů používá nějakou formu ochrany proti virům a malwaru. Rovněž data si šifruje a pravidelně zálohuje zhruba jen desetina uživatelů," konstatuje **Lukáš Pelc,** senior technik společnosti **ServisNaklik.cz**, která zajišťuje servis výpočetní techniky domácím uživatelům.

Mobily a tablety jsou snadno zpeněžitelnou kořistí

Podle nejnovějšího výzkumu Media projekt v **Česku používá mobil nebo tablet 41,7 % populace, tedy 3,7 milionu obyvatel***. To je podle Národního centra bezpečnějšího internetu pro podvodníky již dostatečné lákadlo, aby **realizovali sofistikovanější útoky**. Zatím se totiž viry a malware na mobilních zařízeních šíří pomaleji než na stolních počítačích, ale začínají se objevovat i poměrně nebezpečné útoky. „Po instalaci malwaru se uživateli například začnou nepozorovaně **odesílat z telefonu SMS zprávy na drahé placené linky**," dodává Jiří Palyza z NCBI.

Nová generace malwaru a virů se nezaměřuje na smazání dat, ale hlavně na **převzetí kontroly zařízení a jeho zneužití**. „Ve většině případů se viry či malware snažily uživatele **přimět k platbě pod výhrůžkou pokuty** od policie nebo jiné záminky. Často vir zablokuje počítač a neznalý uživatel ho neumí obnovit a nechá ho přeinstalovat, čímž nepřímo o všechna data přijde," popisuje běžnou praxi Lukáš Pelc z firmy ServisNaklik.cz.

Těmito útoky mohou být **uživatelé okradeni o stovky či tisíce korun měsíčně**. Je ale jen otázkou času, než nějaká zločinecká organizace na tato zařízení podnikne **masivní útok**. „Útočníci budou pravděpodobně vyzývat k instalaci podvodného zákeřného softwaru, jehož účelem bude podvodně získat hesla a přístup k bankovním účtům ovládaným z mobilního zařízení," varuje Ivan Janoušek.

Uživatelé si svá mobilní zařízení mohou chránit velmi podobně jako osobní počítač. „Samozřejmostí by měla být instalace zabezpečovacího softwaru a vyvarování se nebezpečného chování, jakým je například instalace neznámých aplikací, přílišná důvěřivost či volba jednoduchých hesel," doporučuj Jiří Palyza z NCBI.

Digitální vydírání je novou bezpečnostní hrozbou

Nehrozí pouze sofistikované útoky, ale i **různé formy on-line vydírání**. Mobilní zařízení lidé běžně využívají pro **osobní a někdy i velmi intimní komunikaci**. „Řada uživatelů používá fotoaparát v mobilu namísto klasického. Mnozí se neváhají fotit i ve velmi diskrétních či intimních momentech, tyto fotky mohou být zneužity k vydírání. To se týká nejen domácích uživatelů, ale i firemních. Zejména společensky vysoce postavené osoby pak mohou být snadno vydíratelné," čerpá ze své praxe soudní znalec Ivan Janoušek.

Vyděrači navíc nemusí disponovat choulostivými fotografiemi. Stačí, aby **zcizili nezálohovaná data, například fotografie**, o které nechtějí majitelé mobilu či tabletu přijít. Řada uživatelů si **hodnotu informací uvědomí až v okamžiku ztráty** a pro záchranu dat jsou ochotni udělat téměř cokoli: „Tedy i vyděračům zaplatit a nechat se i jinak vydírat. Lidé přistupují ke své digitální identitě mnohdy velmi lehkovážně a dělají věci, které by mimo digitální svět nikdy neudělali. Ledabylost může mít v případě zneužití či ukradení identity katastrofální důsledky," varuje Jiří Palyza z NCBI.

Se ztrátou mobilního zařízení totiž uživatelé obvykle **ztratí i přístup k oblíbeným komunikačním systémům** typu Facebook, Twitter nebo přístupy k firemním systémům, minimálně e-mailu. „Podvodníkům pak stačí jen **pár hodin na zcizení identity a zablokování přístupu ke službám**. Jejich odblokování je náročné a třeba i několik dní nemůže okradený majitel služby využívat. Během této doby se však může zloděj vydávat za dotyčnou osobu a způsobit jí značné škody," uzavírá soudní znalec Ivan Janoušek.

Více informací poskytne:

Jan Hlaváč, mediální zástupce společnosti APOGEO Esteem
tel.: (+420) 777 076 760, jan.hlavac@mediakom.cz

O společnosti APOGEO Esteem, a.s.

Znalecký ústav APOGEO Esteem, a.s. je součástí poradenské skupiny APOGEO Group. Znalecký ústav disponuje jedním z nejširších rozsahů znaleckých oprávnění v České republice pro obor ekonomika a kybernetika, jež uděluje Ministerstvo spravedlnosti České republiky. Více informací je k dispozici na www.apogeo.cz

O Národním centru bezpečnějšího internetu (NCBI)

NCBI je neziskové nevládní sdružení založené v roce 2007. Jeho posláním je přispívat ke zvýšení bezpečnosti užívání internetu, moderních informačních a komunikačních technologií, zvyšovat povědomí uživatelů o jejich kladech a možných nebezpečích, přispívat k osvojování etických norem v on-line prostředí, napomáhat předcházení a snižování možných sociálních rizik spojených s jejich užíváním. Hlavním cílem sdružení je vytvořit a provozovat odborné pracoviště pro osvětu, vzdělávání a ochranu uživatelů před ilegálním a ohrožujícím obsahem na internetu. Více informací je k dispozici na www.ncbi.cz.