Ochranu dat podceňujeme. Napadnout přitom jde i elektronické občanky

Moravské hospodářství | 17.12.2018 | Rubrika: eGovernment | Strana: 8 | Autor: Michaela Římanová | Téma: Masarykova univerzita, vysoké školy

KAŽDOU HODINU JE VE SVĚTĚ UKRADENO NEBO ZTRACENO VÍC NEŽ MILION DATOVÝCH ZÁZNAMŮ. NEJVÍCE Z TĚCHTO PŘÍPADŮ SE ODEHRÁLO V SEVERNÍ AMERICE A VE VÝCHODNÍ ASII. PROBLÉM OCHRANY DAT SE ALE TÝKÁ I ČESKÉ REPUBLIKY. V OHROŽENÍ JSOU NEJEN DOMÁCÍ FIRMY, ALE VÝRAZNĚ TAKÉ STÁTNÍ SPRÁVA, KTERÁ NAKLÁDÁ S VYSOCE CITLIVÝMI ÚDAJI.

Dvě třetiny Čechů vůbec nešifrují data při internetové komunikaci nebo na externích discích. A to dokonce ani tehdy, pokud jde o důvěrné iremní informace. Plyne to z průzkumu, který uskutečnila bezpečnostní společnost ESET ve spolupráci s největší českou internetovou společností Seznam.cz. „Lidé obecně nešifrují ze dvou hlavních důvodů: buď neví, jak se to dělá, nebo jsou přesvědčeni, že to nepotřebují. Jeden z těchto dvou důvodů uvedlo 77 procent z těch, co nešifrují," konstatuje Václav Zubr, bezpečnostní expert české pobočky společnosti ESET.
Dan Rosendorf ze společnosti ICZ připomíná, že zájem o bezpečnost přitom roste. U veřejnosti, ale i ze strany státu a organizací. „Typy hrozeb, se kterými se setkáváme, se zásadně liší podle systému a zákazníka. U menších klientů jsou to stále především necílené hrozby běžného malwaru, ransomwaru a podobně. U zákazníků s hodnotnějšími daty či systémy pak jde jak o běžné APT (přetrvávající pokročilé hrozby, advanced persistent threats - pozn. red.), tak dnes stále více i o útoky na nižších úrovních firmwaru, či dokonce hardwaru," upřesňuje Rosendorf.
Největší ohrožení bezpečnosti šifrování představují takzvané implementační slabiny v samotných systémech. Loni například informatici z **brněnské** Masarykovy univerzity odhalili zranitelnost bezpečnostních čipů německé firmy Inineon Technologies. To zasáhlo Slovensko, protože právě tento čip používá místní státní správa pro autentizaci a v občanských průkazech. Totéž se stalo e-governmentu v Estonsku a poté, co se věc rozkřikla, se přišlo na to, že stejné čipy používají i ve Španělsku.
Tématem roku 2018 je také GDPR, tedy Obecné nařízení o ochraně osobních údajů z dílny Evropské komise. „Díky GDPR se řada organizací začala zabývat ochranou osobních údajů a informační bezpečností obecně. A to je dobře. Kromě krádeže či zneužití informací hrozí i zneužití zařízení a infrastruktury," říká Miroslav Nečas ze společnosti Tovek a dodává, že se stále více pozornost útočníků zaměřuje na mobilní telefony a brzy přijde na řadu i nositelná elektronika.
" Šifrovat, šifrovat, šifrovat!
Ale jak?

Jednou z možností ochrany dat před zneužitím je šifrování, které může mít zásadní význam při zcizení mobilní techniky. Využívají vůbec podniky tuto možnost dostatečně a změnila se situace v souvislosti s direktivou GDPR? Podle Dana Rosendorfa je snaha o šifrování dat často nadužívána. „Mnoho podniků ho vidí jako jakousi magickou pilulku, která jim vyřeší všechny problémy. Přitom vůbec neuvažují o tom, jak a proč ho nasazují. U přenosné techniky je šifrování samozřejmě zásadní, hodnotné a často užívané. Ale i zde mnohdy vidíme nasazení provedená velice špatně," říká Rosendorf a doplňuje, že vždy je třeba uvažovat o problému komplexně. Zašifrovaný počítač, u kterého je klíč pro šifrování odvozen od hesla, jež uživatel zároveň používá pro přístup k dalším čtyřem službám i mimo firmu, není ideálně chráněn.
„Podle GDPR, které platí od letošního května, musí firmy jakoukoli ztrátu či odcizení nešifrovaných osobních dat hlásit Úřadu pro ochranu osobních údajů. Pokud tak neučiní a únik dat se prokáže, riskují citelnou sankci," upozorňuje Zubr a dodává, že pozor by si měly dávat především české pobočky nadnárodních společností, protože případnou sankci by úřad vypočítával z ročního obratu mateřského koncernu.
Většina menších a středních irem nemá zavedeny procesy pro pravidelné testování zranitelností využívaných systémů a už vůbec chybí návazný proces jejich eliminace a opětovného testování," upřesňuje bezpečnostní specialista Jan Pawlik ze společnosti Trusted Network Solutions, který se systematicky věnuje ochraně dat a řízení informační bezpečnosti.

***

„Pozor na únik dat by si měly dávat především české pobočky nadnárodních společností, protože případnou sankci by úřad vypočítával z ročního obratu mateřského koncernu.