BEZPEČNOST DAT UCHOVÁVANÝCH V ELEKTRONICKÉ PODOBĚ

Při uchovávání dat v elektronické podobě, tedy na pevných discích počítačů, sdílených discích, přenosných zařízeních jako např. flash disky, externí disky nebo u externích poskytovatelů datových úložišť je nutné dbát na jejich bezpečnost stejně jako u dat, které jsou zachyceny na listinách. U elektronicky uchovávaných dat je situace složitější proto, že kromě přímého přístupu neoprávněné osoby k danému zařízení hrozí únik dat prostřednictvím dálkového přístupu přes internet.

Pokud dojde k úniku osobních údajů, které mohou někoho poškodit, hrozí riziko na jedné straně ze strany správních úřadů, které mohou uložit v případě nedostatečných bezpečnostních opatření pokutu, na druhé straně v podobě nároků na náhradu škody způsobené osobám, jejichž údaje byly zneužity.

Přestože únik dat v důsledku nezákonného jednání osob, např. hackerského útoku, nelze nikdy zcela vyloučit (stejně jako např. krádež listin), je možné při dodržení několika jednoduchých opatření takové riziko minimalizovat.

+ Heslo

Počítač je nutné mít vždy zabezpečený heslem, které nelze bez jeho znalosti uhodnout. Nevhodná jsou tedy jména, data narození apod. Heslo je bezpečnější, pokud obsahuje číslice i písmena nebo jiné znaky. Je nutné mít na paměti také nastavení počítače tak, aby se po přiměřené době nečinnosti obrazovka uzamkla a pro odemknutí opět bylo nutné zadat heslo – pro případ, že by se neoprávněné osoba dostala k počítači, který je již zapnutý. Každá osoba, která počítač užívá, by měla mít samostatný profil zabezpečený svým heslem, aby bylo možné zajistit přístup pouze oprávněných osob k určitým údajům.

+ Aktualizace softwaru

Běžně používaný softwaru, zejména na úrovni operačních systémů (nejčastěji Windows), pravidelnými aktualizacemi reaguje mimo jiné na bezpečnostní hrozby (např. viry, malware, ransomware). Je proto potřeba navrhované aktualizace pravidelně instalovat a nechávat zapnutý antivirový software.

+ Bezpečný software

Ne každý software dostupný ke stažení na internetu je bezpečný. Některý může obsahovat viry nebo jiné hrozby, které mohou ohrozit bezpečnost dat v počítači, na který jsou nainstalovány. Na počítače obsahující jakékoli osobní údaje je proto nutné instalovat pouze běžně užívaný software, nikoli software, který uživatel nezná. U programů, které přímo osobní údaje jakkoli zpracovávají (např. účetní software), je nutné používat jen bezpečnostně prověřený software, který bezpečnost dat garantuje. Takový software zpravidla vyžaduje přihlášení jménem a heslem, které je nutné nastavit stejně jako heslo k počítači.

+ E-mail

Zdarma poskytované e-mailové služby zpravidla negarantují příliš vysokou bezpečnost dat, která jsou přes ně posílána. Pro odesílání osobních údajů e-mailem je proto nutné vždy užívat e-mailovou adresu zajištěnou ze strany CASD. V případě zasílání údajů, které jsou zvlášť citlivé (např. mzdy, údaje o finančních záležitostech, seznam členů církve) je pak vhodné takové údaje posílat v zaheslovaném souboru v některém z běžně užívaných archivů

(např. WinZip). Jako obrana před útoky na bezpečnost počítačů prostřednictvím e-mailů je nutné otevírat e-maily, a zejména jejich přílohy, jen od známých odesílatelů, které neobsahují žádný podezřelý text.

+ Cloudová úložiště

Pro ukládání dat je možné užívat i tzv. cloudové služby, kdy jsou data nahrávána na servery poskytovatele a následně mohou být přístupná z více počítačů (např. Google Disk, Dropbox). Je ale potřeba zvážit úroveň zabezpečení takových úložišť u třetích osob, zdarma poskytované služby opět příliš vysokou úroveň zabezpečení negarantují. K ukládání dat obsahujících jakékoli osobní údaje je proto vhodné používat výhradně Google Disk zajištěný pro tyto účely ze strany církve.

+ Externí úložiště

V případě používání externích disků nebo flash disků pro přenášení dokumentů obsahujících jakákoli citlivá data a osobní údaje je nutné pro případ ztráty nebo odcizení tohoto zařízení používat zaheslované archivy stejně jako v případě e-mailu.

+ Sociální sítě

Na sociální sítě nebo podobné webové služby jsou nejčastěji nahrávány fotografie ve spojení se jmény osob. Pokud jsou takové fotografie prezentovány veřejně, je nutné, aby s tím zobrazené osoby prokazatelně souhlasily, a také, aby bylo zaručeno, že tyto fotografie nebudou zneužity k jiným účelům, než ke kterým byly určeny. Pokud jsou určeny ke sdílení jen s určitým okruhem osob, musí sociální síť umožňovat takové nastavení. Musí tako garantovat bezpečnost dat uživatelů, které má ve své dispozici. Je možné za dodržení podmínky souhlasu dotčených osob a správného nastavení přístupu používat např. Facebook nebo Instagram. Účet musí být proti zneužití také zabezpečený heslem.

Na závěr je nutné připomenout, že pokud jsou data nahrávána do jakéhokoli programu, který je ukládá jinam, než do počítače, na kterém je nainstalován, provozovatel tohoto softwaru je v pozici zpracovatele osobních údajů. Za bezpečnost dat u zpracovatelů vždy odpovídá správce, tedy ten, komu byly jednotlivými osobami údaje poskytnuty. Se zpracovatelem je nutné mít o zpracování osobních údajů uzavřenou smlouvu – poskytovatelé bezpečných softwarů toto rovnou nabízejí ve svých smluvních podmínkách.

V případě, že dojde k situaci, kdy elektronicky uchovávaná data i přes veškerá opatření uniknou, je nutné porušení bezpečnosti řešit tak, aby se podařilo, pokud možno, škodám předejít, nebo je alespoň minimalizovat. V takovém případě prostřednictvím tajemníka svého sdružení kontaktujte pověřence pro osobní údaje za účelem nalezení nejlepšího řešení.