ZABEZPEČENIE POČÍTAČOV A DÁT

(SPRACÚVANIE OSOBNÝCH ÚDAJOV V CIRKEVNÝCH AUTOMATIZOVANÝCH INFORMAČNÝCH SYSTÉMOCH)

Tento dokument nadväzuje na technologické informácie ohľadom ochrany interných informačných údajov v oblasti ochrany osobných údajov uvedené v dokumente:

Interné informačné systémy
na webovej stránke Ochrana osobných údajov (gdpr.kbs.sk) → Technologické informácie

Osobné údaje sa vo veľkej miere spracúvajú prostredníctvom automatizovaných informačných systémov (informačných a komunikačných technológií) i v prostredí Rímskokatolíckej cirkvi, Gréckokatolíckej cirkvi a právnických osôb, ktoré si svoju právnu subjektivitu od nich odvodzujú. Bezprostrednou súčasťou, resp. nástrojom interných automatizovaných informačných systémov cirkvi sú osobné počítače, prenosné zariadenia a dátové úložiská[1] používané internými pracovníkmi Cirkvi.

Treba zabezpečiť, aby aj tieto informačné prostriedky spĺňali podmienky pre spracúvanie osobných údajov dotknutých osôb v automatizovaných informačných systémoch v súlade so Zákonom 18/2018 Z.z. o ochrane osobných údajov a Nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov.

1. Prístup k zariadeniam a dátovým úložiskám

Výpočtovú techniku a úložiská, na ktorých sa nachádzajú/spracúvajú osobné údaje, treba chrániť takým spôsobom, aby neprišlo ku kompromitácii osobných údajov[2].

1.1. Fyzický prístup

Umožniť fyzický prístup k výpočtovej technike a úložiskám, na ktorých sa nachádzajú, resp. spracúvajú osobné údaje, len povereným osobám a zabrániť odcudzeniu/strate techniky a úložísk – napr. počítač umiestnený v uzamykateľnej kancelárii; prístup verejnosti do kancelárie s počítačom len za prítomnosti poverenej osoby; DVD/CD alebo usb disk/kľúč so zálohami uložený v trezore/uzamykateľnej kovovej skrini, resp. je použité dostatočne silné šifrovanie obsahu; ak sa notebook s osobnými údajmi nachádza na mieste prístupnom verejnosti, je mechanicky chránený proti odcudzeniu[3] a pod.

1.2. Šifrovanie dát

Dátové úložiská a výpočtová technika (notebooky, tablety, mobily) s osobnými údajmi, ktoré sú prenášané mimo zabezpečených priestorov, je treba, aby boli šifrované!

1 Napr. pamäťové karty, usb klúče, usb disky, DVD/CD,...
2 Pod kompromitáciou sa rozumie akýkoľvek únik, prezradenie, odpočúvanie, či zneužitie dát.
3 Tzv. zámok pre notebook – Kensington lock/Kensington Security Slot.

Je možné použiť šifrovanie celého disku/média, alebo len šifrovanie osobných údajov.

Šifrovanie je vhodné, no nie nutné, použiť aj na zariadenia a úložiská, ktoré sa nachádzajú v zabezpečených pracovných priestoroch. Avšak – ak je použitý operačný systém, ktorý nevie nastavovať prístupové práva k dátam (a tým zablokovať prístup k osobným údajom pre nepovolané osoby, ktoré by tiež mali k počítaču prístup, aj keď pod iným menom a heslom než poverená osoba), na spracúvanie osobných údajov musí byť použitá taká aplikácia (softvér), ktorá zabezpečí šifrované uloženie osobných údajov.

Nástroje pre šifrovanie diskov a dát:

- Nástroje systémovej podpory šifrovania diskov v rámci jednotlivých operačných systémov
  - GNU/Linux[4] - LUKS, dm-crypt,...
  - MS Windows[5] - Bitlocker
  - MacOS X - FileVault
- Alternatívne nástroje pre šifrovanie diskov
  - VeraCrypt: softvér na šifrovanie diskov počítača (multiplatformný: MS Windows, Mac OS X, GNU/Linux)
- Nástroje pre šifrovanie súborov (všetky uvedené sú multiplatformné)
  - EncFS – nástroj pre transparentné šifrovanie súborov na disku počítača
  - Aescrypt – nástroj pre šifrovanie súborov a dát (vhodné i na posielanie dát)

2. Prístup k obsahu – prístup k osobným údajom

Prístup priamo k osobným údajom i prístup k aplikáciám spracúvajúcim osobné údaje treba chrániť takým spôsobom, aby neprišlo ku kompromitácii osobných údajov.

2.1. Prihlasovanie sa do systému

Treba zabezpečiť identifikáciu, autentifikáciu a autorizáciu pri spracúvaní osobných údajov – t.j. meno, heslo a prístupové práva.

Identifikácia: každá poverená osoba má svoj vlastný účet, t.j. svoje vlastné prihlasovacie meno.
Autentifikácia: prístup poverenej osoby je chránený heslom, t.j. každý účet má vytvorené dostatočne silné heslo[6]. **Pozor: biometrický údaj sám o sebe nenahrádza heslo!**
Autorizácia: poverená osoba a len poverená osoba/y má dostatočné prístupové práva pre prístup a spracúvanie osobných údajov, t.j. do súborov, či k databázam s osobnými údajmi a do aplikácií spracúvajúcich osobné údaje sa používateľ dostatne len na základe svojho zaradenia a v rozsahu svojich oprávnení[7].

4 Väčšina moderných distrinúcií GNU/Linuxu ponúka priamo pri inštalácii možnosť zapnúť šifrovanie diskov.
5 Niektoré edície MS Windows šifrovanie Bitlocker nepodporujú. V týchto prípadoch je možné využiť alternatívny VeraCrypt (z pohľadu výberu nezávislého šifrovania môže byť VeraCrypt na MS Windows aj prvou voľbou).
6 Pre zvýšenie bezpečnosti v systémoch, ktoré to podporujú, je možné využiť dvojfaktorovú autentifikáciu (2FA).
7 V komplexných informačných systémoch ide o správu identít (IdM) a riadenie prístupu na základe rolí (RBAC) – viď dokument Interné informačné systémy. Jednoducho povedané: role znamenajú, že jednotliví používatelia môžu mať rôzne práva na základe ich pracovného zaradenia.

Prístup do zariadenia na základe indetifikácie a autentifikácie je nutnou podmienkou pre spracúvanie osobných údajov.
Nastavenie prístupových práv k osobným údajom len pre poverené osoby je nutnou podmienkou pre spracúvanie osobných údajov.

2.2. Aplikácie spracúvajúce osobné údaje[8]

Prístup do aplikácie musí byť riadený na základe prístupových práv (meno a heslo/2FA) a prípadne aj rolí (nastavený rozsah prístupu k spracúvaným osobným údajom) per používateľ (nie teda prístup zdieľaný viacerými používateľmi, napr. cez spoločné meno a heslo).

V jednoduchých prípadoch[9] je možné nahradiť prihlasovanie do aplikácie len prihlasovaním sa do operačného systému.

3. Monitoring a logovanie

Ide o ukladanie záznamov o tom, kto a kedy s osobnými údajmi pracoval, prípadne aké operácie vykonával.

Na úrovni operačného systému treba ukladať minimálne záznamy o prihlásení a odhlásení používateľa.[10]

Na úrovni aplikácie – ak umožňuje prihlasovanie – treba ukladať záznamy o prihlásení a odhlásení používateľa. Je vhodné, ak aplikácia naviac dokáže monitorovať a ukladať aj vykonané operácie pri spracúvaní osobných údajov.[11]

4. Zabezpečenie zariadení pred škodlivým kódom

Jedným z najrozšírenejších spôsobov[12] kompromitácie výpočtovej techniky je zneužitie chýb v informačných systémoch prostredníctvom škodlivého kódu.

Základné informácie o zabezpečení počítača spolu s praktickými radami je možné nájsť napr. na stránkach Christ-Net.Sk: Zabezpečenie počítača.

Komplexné informácie o kybernetickej bezpečnosti, zabezpečení zariadení, škodlivých aktivitách, **bezpečnostných návykoch** a postupoch, ako sa chrániť, sú uvedené na stránkach Národného bezpečnostného úradu, Národnej jednotly SK-CERT v časti Rady pre verejnosť.

8 Napr. matričný softvér, personalistika, služby portálu ecclesia,...
9 Napr. lokálna práca s osobnými údajmi v MS Word, lokálny jednoužívateľský matričný systém, účtovníctvo a pod.
10 V súčasnosti všetky bežne používané operačné systémy z rodín MS Windows, GNI/Linux, MacOS X,... majú toto logovanie zapnuté.
11 Napr. spisová služba tribunálu portálu ecclesia.sk má túto funkcionalitu plne implementovanú.
12 Ďalšími sú sociálne inžinierstvo a nekalé/nezodpovedné konanie používateľa.

5. Riešenie incidentov

V prípade podozrenia na akúkoľvek kompromitáciu zariadení spracúvajúcich osobné údaje v rámci Katolíckej cirkvi, či v prípade akejkoľvek straty a krádeže dátových úložísk s osobnými údajmi **je treba čo najskôr kontaktovať Zodpovednú osobu** (DPO[13]) Katolíckej cirkvi, ktorá je uvedená na webovej stránke Ochrana osobných údajov (gdpr.kbs.sk) → Zodpovedná osoba.

S pomocou DPO bude možné klasifikovať incident a vykonať prípadné potrebné kroky pre ochranu osobných údajov, informovanie dotknutých osôb a splnenie legislatívnych požiadaviek Zákona o ochrane osobných údajov.

6. Jednoduché pravidlá pre zabezpečenie zariadení a dátových úložísk

Zariadenia spracúvajúce osobné údaje:

- stolný počítač v zabezpečenom priestore (napr. kancelária, do ktorej bez prítomnosti poverenej osoby iní nemajú prístup);
- notebook/tablet v zabezpečenom priestore (napr. kancelária, do ktorej bez prítomnosti poverenej osoby iní nemajú prístup) s mechanickým zámkom (Kensington lock);
- notebook/tablet/mobil mimo zabezpečeného priestoru: so šifrovaním osobných údajov, resp. celého disku/úložiska;
- prenosné dátové úložiská, na ktorých sa osobné údaje prenášajú mimo zabezpečeného priestoru, musia byť šifrované;
- záložné médiá/dátové úložiská sú uložené na bezpečnom mieste.

Softérové nastavenie na zariadeniach

- každý používateľ sa prihlasuje svojím menom/heslo, prípadne rozšírenou autentifikáciou (2FA, viď vyššie);
- v operačnom systéme/aplikácii sú nastavené prístupové práva k osobným údajom;
- je zapnuté autentifikácia (prihlasovanie) používateľov do aplikácií spracúvajúcich osobné údaje;
- je zapnuté ukladanie záznamov o prihlasovaní používateľov, prípadne o jednotlivých úkonoch pri spracúvaní osobných údajov;
- sú aplikované základné pravidlá zabezpečenia zariadení proti škodlivému kódu a informačnej kriminalite.

13 Data Protection Officer.