FAKULTA
APLIKOVANÝCH VĚD
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI

Katedra informatiky a výpočetní techniky

Pokyn vedoucího katedry č. 2VK/2018

Zacházení s citlivými údaji na Sekci pro informační technologie

1. Úvodní ustanovení

Členové KIV a NTIS-P2 pracují mj. s osobními údaji lidí (viz GDPR), údaji podléhajícími obchodnímu tajemství (viz smluvní výzkum a NDA) a znalostmi na špičce poznání využitelnými pro inovace (viz základní výzkum). Takovéto údaje jsou *citlivé* v tom smyslu, že jejich únik do nepovolaných rukou – bez souhlasu toho, kdo je poskytnul – může znamenat významný problém právní, finanční, morální a praktický.

Pro vhodnou ochranu citlivých informací, vč. případů práce mimo kancelář, stanovuji pro všechny zaměstnance a doktorandy Sekce následující pravidla a doporučení.

2. Základní zásady

- Nejsem-li v kanceláři, nemá v ní být ani nikdo jiný (kromě zaměstnanců) a jsou zavřené dveře.
- Na stole apod. nenechávám volně ležet papíry, dokumenty, disky apod. s citlivými údaji; používám šanony ve skříni apod. případně se o uložení dokumentů dohodnu na sekretariátu.
- Citlivé údaje nedávám na web s volným přístupem (např. výsledky písemek na home.zcu.cz, smlouvy na Dropbox, fotky na Facebook); používám courseware.zcu.cz, AFS, gapps.zcu.cz, ap.
- Mobilní zařízení, kde jsou citlivé údaje, mám velmi dobře zabezpečená; stacionární zařízení (PC apod.) mám chráněná proti volnému přístupu; oboje viz následující oddíl.
- Když nevím nebo si nejsem jistý/á, zeptám se tajemnice katedry a/nebo technické skupiny.

3. Používání notebooků, PC a dalších zařízení

Následující body platí *povinně* pro zařízení, u kterých je předpoklad, že na nich budou citlivé údaje ukládány či zpracovávány (a to jak zařízení univerzitní tak v osobním vlastnictví, používaná pro práci). Pro ostatní zařízení a účely (např. notebooky z poolu, speciální měřící PC, apod.) platí *přiměřeně*.

- Mít zapnuté a spouštěné automatické aktualizace systému, příp. antivir (povinně pro OS Windows) a správně nastavený firewall, pro všechna mobilní zařízení (telefony a tablety), notebooky, pracovní stanice, virtuální servery používané pro práci.

- Mít vypnutý vzdálený přístup, nebo případně povolený jen z IP adresního rozsahu ZČU a pro přístup na zařízení z vnější sítě používat VPN (viz http://support.zcu.cz/index.php/VPN).
- Používat přihlášení s heslem, nikoli automatické přihlášení, pro notebooky a mobilní zařízení navíc heslo pro probuzení ze spánku / uzamčené obrazovky. Je-li to možné, nastavit uspání počítače po cca 2 hodinách.
- Používat silná hesla (viz např. https://www.blueghost.cz/clanek/10-pravidel-bezpecnost-hesel/ , https://devel.cz/otazka/co-je-silne-heslo#answer-16252).
- Mít puštěné pravidelné zálohování dat, pokud možno na úložiště spravované technickou skupinou KIV nebo CIV ZČU (kde je garance obnovy dat).
- Používat šifrování disku (full-disc encryption) – zejména důležité na mobilních zařízeních a noteboocích, kde je předpoklad práce s citlivými údaji.
- Používat šifrování flash disků a dalších přenosných úložišť, která se používají pro (dočasné) ukládání citlivých údajů.
- Nepoužívat k ukládání citlivých údajů soukromé účty na úložištích typu Dropbox apod., veřejné služby typu github.com, ani notebooky v poolu a stanice ve výukových laboratořích.
- Neposílat citlivé údaje emailem, zejména na účty mimo @zcu.cz, pokud je lze předat jinak.
- Nepoužívat lokální účty typu demo/demo, test/test atp. (tj. „pokusné se slabým heslem“).
- Ihned hlásit technické skupině a vedoucímu katedry jakýkoli problém (i podezření na něj) na zařízení, spravovaném virtuálním serveru, nebo na počítači v laboratoři, pokud by problém mohl vést ke ztrátě nebo úniku citlivých údajů.

Na noteboocích je doporučeno mít uskladněna jen data aktuálně potřebná k práci (pro cca daný semestr/rok), ostatní data mít na garantovaném úložišti KIV/ZČU s přístupem jen z VPN.

Výukové laboratoře a specializovaná zařízení vč. PC

Pro výukové laboratoře je bezpečnost řešena Provozním řádem vč. toho, že vyučující a správci laboratoří mají povinnost stav laboratoře kontrolovat.

Pro specializovaná zařízení a laboratoře platí pravidla dle Provozního řádu, povinnost aby laboratoř měla jasně určeného správce, aby zařízení měla nálepku s IP adresou a jménem správce, a vše z bodů výše. Dále je nutné, aby o správci a o umístění zařízení věděla technická skupina KIV a sekretariát.

4. Doporučení pro práci s citlivými údaji

Upozornění: Osobním údajem je *jakákoliv* informace týkající se určeného nebo určitelného [člověka]. Člověk je (z hlediska přístupu k jeho osobním údajům) určitelný jakýmkoli primárním nebo složeným klíčem, např. rodným číslem, os.č. studenta v kombinaci s daty veřejně dostupnými ve STAGu, twitter/facebook přezdívkou ve spojení s plným jménem na profilu, kombinací příznaků v datové sadě („malý černovlasý muž s červeným Porsche v Horních Kotěhůlkách“).

Co *není* osobním údajem: potenciálně vůbec nic. Nicméně, údaje neodpovídající duchu výše uvedeného mají šanci být považovány za bezpečné. Např. dobře anonymizovaná data v kvalitní datové sadě, souhrnné statistiky, data dostupná z veřejných zdrojů, apod.

Vybraná doporučení

- Neskladovat, co nutně nepotřebuji; skartovat, nikoli házet do koše (platí i pro CD apod.).
- Dávat výsledky testů, zkoušek apod. na Courseware na stránku předmětu dostupnou jen po přihlášení (tj. ne O předmětu) s použitím portletu pro zobrazení CSV, s klíčováním přes os.č.
- Pro sdílení citlivých údajů používat gapps.zcu.cz disk nebo AFS, pokud je zpřístupněno pouze konkrétním uživatelům ze ZČU a pokud tito uživatelé nemohou soubor/adresář dále dávat ke sdílení a dostanou informaci, že jde o citlivé údaje a že s nimi tak mají nakládat.

- Používat pro podobné účely systém Redmine na https://forge.kiv.zcu.cz:3443/ , jen pokud je příslušný projekt zpřístupněn pouze jasně definovaným uživatelům ze ZČU a pokud tito uživatelé dostanou informaci, jak s údaji mohou nakládat.
- Předat fyzicky (nahrát z flash disk pod dohledem) a hned z dočasného úložiště (flash disk) smazat, jen pokud je takto zpřístupněno pouze jasně definovaným uživatelům ze ZČU nebo členům projektového týmu a pokud tito uživatelé nemohou data dále dávat ke sdílení a dostanou informaci, že jde o citlivá data a že s nimi tak mají nakládat.
- Údaje neprověřenému nebo podezřelému zájemci nesdělovat/nepředávat a ohlásit vedoucímu pracoviště, kdo má o informace zájem.
- Vědět, že existuje, a používat http://support.zcu.cz/index.php/Kategorie:Bezpe%C4%8Dnost a http://support.zcu.cz/index.php/GDPR .

5. Závěrečná ustanovení

Technická skupina KIV má dále pravomoc náhodně i systematicky kontrolovat míru zabezpečení na všech výše popsaných typech zařízení, vzdáleně i fyzicky, a povinnost ve spolupráci s dotyčným zjištěné nedostatky bezodkladně odstranit. Zařízení s přetrvávajícími problémy bude fyzicky odebráno.

V Plzni, dne 25.5.2018

doc. Ing. Přemysl Brada, MSc. Ph.D.
vedoucí katedry