Bezpečnost automatizovaného zpracování dat

**Vymezení problému**

* hlavní problémem je bezpečnost zpracování dat automatizačními nástroji
* klíčové podoblasti
  + analýza současných RPA řešení a jejich přístupů k bezpečnosti dat, analýza jednotlivých příruček a návodů “jak implementovat do firmy RPA” dostupných na internetu
  + bezpečnost zpracování dat v českém právním prostředí
    - zákon o ochraně osobních údajů
    - GDPR
    - zákon o kybernetické bezpečnosti?
  + procesní problémy

**Účel a cíle projektu**

Cílem této práce je analyzovat bezpečnostní rizika při zpracování dat automatizovanými nástroji a následně navrhnout vhodná bezpečnostní opatření. V práce je brán zřetel na právní hlediska, kyberbezpečnost a procesní bezpečnost.

* hlavním cílem je analyzovat rizika a pokusit se je vyřešit nebo aspoň zmírnit jejich dopady
* to se dá dělat různými cestami, proto se zaměříme nejvíce na řešení ve smyslu aplikace mechanismů z informatiky
* dalším cílem je pomoci firmám zjistit jestli se tyto problémy zrovna pro ně vyplatí řešit
* zanalyzovat, jak chránit různá data různé citlivosti podle prostředí kde jsou uchovávána
* má to smysl řešit hlavně kvůli finančním dopadům (pokuty, úniky konkurenci) a i etickým dopadům a poškozením image firmy

# Rámcová osnova

1. Možnosti automatizovaného zpracování dat.
2. Analýza bezpečnostních rizik při zpracování dat automatizovanými nástroji.
3. Praktická implementace vybraného bezpečnostního opatření.

# Úvod - ukázka

Není to tak dávno, co pojem automatizace představoval jen zavádění robotů a automatických procedur do továren a byl spojen pouze s průmyslovým sektorem. Dnes si bez těchto technologií svět nedokážeme ani představit. V celém odvětví díky automatizace skokově vzrostla efektivita práce a klasické ruční manufaktury, které předtím existovaly, už téměř nikde v moderním světě nenajdeme.

Poslední dobou můžeme pozorovat nový trend: Stejný proces automatizace, který jsme dříve mohli vidět v průmyslovém sektoru přechází do oblasti služeb, kde se snaží nahradit rutinní kancelářské činnosti a nekreativní, nekvalifikované práce. Nezůstává ale jenom u toho. Velkou automatizační výzvou jsou profese, které potřebují k jejich vykonávání lidskou kreativitu, ale i ty jsou dnes už do jisté míry nahrazovány, za předpokladu, že činnost je dostatečně repetitivní nebo běžná po celém světě.

Zodpovědné automatizační nástroje se v tomto případě označují jako RPA, tedy Robotic Process Automation tools a jsou v současné době na světovém trhu horkým zbožím. Důkazem může být například ukrajinský startup UiPath, který se za poměrně krátkou dobu 4 let stal prvním ukrajinským jednorožcem (startup, která překoná odhadovanou tržní hodnotu 1 miliardu dolarů) (Gheorghe 2018). I v Česku vznikají startupy, které se touto nebo podobnou problematikou zabývají a které aspirují na nejrychleji rostoucí české startupy v historii. Konkrétně společnost Rossum, založená výzkumníky v oblasti umělé inteligence z ČVUT, vybrala v prvním kole financování 2,2 miliardy korun (Tmejová 2021). Cílem této společnosti je umělou inteligencí převádět do digitální podoby “papírové” formy dokumentů, přičemž tento proces je pro úspěšné použití RPA nástrojů klíčový.

Celkově dnešní doba automatizaci velmi nahrává. Kvůli velké nezaměstnanosti je sehnat zaměstnance velmi obtížné a hlavně drahé. A i když se to povede, existuje neustálé riziko, že zrovna když se zaměstnanec naučí způsobům dané firmy a začne být ve vykonávání své práce opravdu efektivní, dostane nějakou jinou zajímavější nabídku jeho vysněné práce za vysněnou mzdu a firma, která si zaměstnance vycvičila může zase začít celý cyklus znovu od začátku.

Krom toho mají informační systémy s integrovanou RPA i další výhody. Především dokáží pracovat se strojovou přesností a místo pro chyby se tak radikálně zmenšuje. Jejich paměť je dokonalá (do té míry do jaké firmy stíhají zvětšovat svá úložiště), vyhledávání jednotlivých informací je téměř bleskové a nová data dokáží zpracovávat 24 hodin denně 7 dní v týdnu. Hlavně ale tyto systémy dokáží najít ve zpracovávaných datech logické vzorce a data dále upravovat tak, aby byly co nejlépe připravené k dalšímu využití. Všichni lidští zaměstnanci se pak mohou soustředit na kreativnější činnosti a řada rutinních záležitostí jim odpadá. To nahrává ke kompletní změně konceptu práce, který dnes již v některých moderních pracovištích můžeme vidět. Pracuje se méně hodin, ale o to efektivněji, chytřeji a v konečném množství odvedené práce i více.

Bohužel implementace RPA do firem nemusí být vždy jednoduchou záležitostí, ač se o to vývojáři těchto řešení snaží. Velká váha totiž padá na architekturu inkriminovaného informačního systému, která musí být dostatečné robustní a flexibilní, aby šlo přidat další kontrolní vrstvu. Zároveň je nutno pamatovat, že všechny změny v nižších vrstvách se logicky budou muset přenášet do budoucna i na RPA, na což musí být firemní IT taky náležitě připraveno. A není to jediný problém. Firemní procesy se musí často kompletně předělat, kompetence se musí změnit a jednotliví stávající zaměstnanci musí projít řadou školení, aby se s novým způsobem práce seznámili. Do toho všeho vstupují nová rizika, která souvisí s větším nasazením informačních technologií. Těmi jsou hlavně závislost na dodavateli technologie, chyby v samotném nástroji (kterých obvykle přibývá se zvětšující se složitostí nástroje) nebo bezpečnostní rizika, která přichází s otevřením systémů novému uživateli s vysokými právy.

Samostatnou kapitolou jsou potom problémy plynoucí z citlivosti samotných dat, s kterými automatizační nástroje pracují. Nejde totiž jen o to, že se soukromé a tajné údaje mohou dostat do cizích rukou. Jde i o samotný zákon, který to může v některých případech zakazovat a sankcionovat. To se v krajních případech dokonce může pro firmu ukázat i jako likvidační. Dalším problémem je únik těchto údajů, jehož pravděpodobnost se kvůli nekontrolovatelnému zpracování dat zvětšuje. Rizik, která se týkají samotných dat a konkrétně jejich zpracováním automatizovanými nástroji je celá řada a konkrétní odborné články zabývající se touto oblastí nejsou dohledatelné. Tato práce se bude v dalších kapitolách zabývat analýzou těchto rizik a návrhem bezpečnostních opatření. Ty budou technického a procesního rázu.