Politechnika Śląska
Wydział Organizacji i Zarządzania

Marta Juszczyk

ROZBUDOWA MODELU AKCEPTACJI TECHNOLOGII DLA POTRZEB BEZPIECZNEGO WYKORZYSTANIA TOŻSAMOŚCI CYFROWEJ W MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTWACH

Rozprawa doktorska napisana pod kierunkiem:
dr. hab. Zbigniewa Pastuszaka, prof. UMCS
i promotora pomocniczego:
dr hab. Izabeli Jonek-Kowalskiej, prof. PŚ

Zabrze, 2017

Abstrakt

W pracy przedstawiono autorski Model Akceptacji Tożsamości Cyfrowej (*Digital Identity Acceptance Model*, DIAM), utworzony na bazie Modelu Akceptacji Technologii (*Technology Acceptance Model*, TAM). W celu jego sporządzenia przeprowadzono kilkuetapowy ciąg działań badawczych.

Na pierwszym etapie badań literaturowych dokonano teoretycznego rozpoznania tematu tożsamości cyfrowych. Źródłem wiedzy były artykuły naukowe, raporty organizacji badających bezpieczeństwo informacyjne oraz rozwój e-gospodarki, a także dokumenty generowane przez przedsiębiorstwa IT, ze szczególnym uwzględnieniem tzw. białych ksiąg.

Wybrano model TAM jako podstawę do objaśnienia czynników powodujących, że pracownicy korzystają z uwierzytelnienia w określony sposób. W celu rozbudowy modelu dokonano krytycznej analizy literatury pod kątem badań nad czynnikami wpływającymi na bezpieczeństwo użytkowania systemów IT (w tym m.in. analiza teorii motywacji oraz dotychczasowego stosowania modelu TAM).

Następnie, w ramach stażu badawczego, prowadzono badania we współpracy z firmą software'ową. Korzystając z doświadczeń pracowników tego przedsiębiorstwa określono, przy pomocy metody delfickiej, problematyczne obszary wpływające na stosowanie tożsamości cyfrowych w warstwie implementacji technicznej, organizacyjnej i przede wszystkim praktyki stosowania tożsamości cyfrowych przez pracowników. Ten ostatni obszar wybrany został do sformułowania problemu badawczego.

W kolejnym etapie opracowano i poddano krytyce ekspertów scenariusz wywiadu otwartego, a następnie przeprowadzono badania z jego wykorzystaniem na grupie 10 menedżerów. Pozwoliły one na poznanie postrzegania przez osoby na kierowniczych stanowiskach celowości i motywacji do stosowania tożsamości cyfrowych w przedsiębiorstwie, opinii na temat różnych sposobów dostępu do danych w systemach informatycznych oraz sposobów na zarządzanie pracownikiem tak, by z powierzonego mu dostępu korzystał w przewidziany sposób. Wyniki wywiadów pozwoliły na zdiagnozowanie potencjalnych luk w sposobie zastosowania tożsamości cyfrowych.

Na podstawie badań z wykorzystaniem metody delfickiej oraz wyników wywiadów otwartych, opracowano kwestionariusz badawczy. Kwestionariusz ten wykorzystano do przeprowadzenia badań wstępnych na ograniczonej próbie pracowników polskich przedsiębiorstw. Badania wstępne dotyczyły:

- Obszaru korzystania z tożsamości cyfrowych z rozszerzeniem o badanie sposobu dostępu do danych (konta indywidualne vs. konta wykorzystywane przez grupę pracowników).
- Postrzegania różnych narzędzi uwierzytelnienia przez pracowników przedsiębiorstw.

Rezultaty badań wstępnych zostały poddane analizie i wykorzystane w przygotowaniu badań właściwych. Badania właściwe przeprowadzone zostały z wykorzystaniem rozbudowanego kwestionariusza badawczego na grupie 202 pracowników małych i średnich przedsiębiorstw. Zbadano:

- organizację dostępu do zasobów systemów informatycznych, a w tym: wdrożenie polityki bezpieczeństwa, rodzaje kont używane przez respondentów oraz stosowane narzędzia uwierzytelnienia dostępu;
- działania użytkownika w kontekście bezpieczeństwa tożsamości cyfrowej, czyli wielowymiarowe wykorzystanie hasła i przedmiotu uwierzytelniającego.
- postrzeganie przez pracownika aktualnie stosowanych rozwiązań, tj. zarządzanie w obszarze kształtowania postaw pracowniczych wobec bezpiecznego uwierzytelnienia, ocenę obecnie stosowanych rozwiązań, określenie preferencji pracowników i porównanie preferencji z obecnie stosowanymi rozwiązaniami;

Drugą częścią badań właściwych było badanie parametrów wstępnego modelu tj. poszczególnych czynników i siły relacji między nimi. W tym celu posłużono się analizą współczynnika Alfa-Cronbacha by określić rzetelność skali i zbadać spójności wewnętrzną pytań. W celu zbadania występowania i siły zależności między elementami modelu postawiono 17 hipotez statystycznych, które badano przy pomocy testów: Chi kwadrat, Chi kwadrat największej wiarygodności oraz korelacji Rang Spearmana.

W wyniku otrzymano 4 obszary modelu DIAM: uniwersalny (DIAM-0), dotyczący uwierzytelnień za pomocą hasła (DIAM-H), przedmiotu (DIAM-P) i biometrii (DIAM-B). Ponadto, zidentyfikowano luki między pracownikami na stanowiskach kierowniczych i wykonawczych.

Podczas analizy wyników badań określono główne 43 zależności (badanie hipotez statystycznych) i 17 wniosków (interpretacja luk i skwantyfikowanego modelu DIAM), na podstawie których sformułowano 20 rekomendacji dla kadry menedżerskiej.
Rekomendacje zostały pogrupowane w następujący sposób:

- projektowanie systemu bezpieczeństwa informacji (6 zaleceń),
- działania i kompetencje przełożonych (5 zaleceń),
- kształtowanie postaw pracowników wobec bezpiecznego uwierzytelniania się (5 zaleceń),
- zalecenia dotyczące zmniejszania oporu pracowników podczas wprowadzania uwierzytelnienia biometrycznego (4 zalecenia).

Marta Juszczyk

16 06 2017