Lublin, dnia 12 kwietnia 2016 r.

URZĄD MIASTA LUBLIN
*Wydział Audytu i Kontroli*
Znak: AK-A-I.1720.5.2016

# NOTATKA Z CZYNNOŚCI SPRAWDZAJĄCYCH

| | |
|---|---|
| **Temat zadania audytowego** | Bezpieczeństwo informacji (BI) w jednostkach organizacyjnych miasta |
| **Adresat zaleceń** | Dyrektor Domu Pomocy Społecznej im. W. Michelisowej w Lublinie |
| **Przeprowadził** | Witold Przeszlakowski, Magdalena Pociecha |

Przedmiotem czynności sprawdzających przeprowadzonych 12 kwietnia 2016 r. była weryfikacja wykonania oraz ocena sposobu wdrożenia i skuteczności realizacji zaleceń wydanych dla Dyrektora Domu Pomocy Społecznej im. W. Michelisowej w Lublinie (DPS) w Sprawozdaniu częściowym z audytu bezpieczeństwa informacji przekazanym w styczniu 2014 r[1]. Podczas zadania audytowego w DPS poziom 3 z 8 testowanych ryzyk oceniono na wysoki.

Dotyczyło to ryzyk:
- braku bezzwłocznej zmiany uprawnień pracowników (administratorów) w przypadku zmiany zakresu zadań lub odejścia z pracy,
- braku aktualnych zabezpieczeń antywirusowych,
- nieterminowego przeprowadzania inwentaryzacji sprzętu i oprogramowania.

W ramach zadania audytowego wydano 9 zaleceń audytowych dotyczących m.in. Wprowadzenia mechanizmów kontrolnych mających na celu obniżenie poziomu ww. ryzyk. W wyniku przeprowadzonych czynności sprawdzających stwierdzono, **że wszystkie z wydanych zaleceń zostały zrealizowane.** Zdaniem audytorów wdrożone w DPS mechanizmy kontroli skutecznie ograniczają testowane ryzyka.

Szczegółowe zestawienie wydanych zaleceń oraz oceny stopnia ich realizacji przedstawiono w poniższej tabeli.

| Lp. | Treść rekomendacji | Status realizacji | Wyniki weryfikacji wdrożenia rekomendacji |
|---|---|---|---|
| 1 | Uzupełnić ewidencję pracowników upoważnionych do przetwarzania informacji o zakres danych, do których przetwarzania zostali upoważnieni (rozróżniając czy dany pracownik ma dostęp do danych w systemie informatycznym czy wyłącznie w formie tradycyjnej), precyzyjnie wskazywać czas trwania dostępu do danych oraz monitorować aktualność przedmiotowych zapisów. | Zrealizowano | DPS posiadał aktualny rejestr osób upoważnionych do przetwarzania danych osobowych. |

1 *Dok. Mdok nr: 35172/01/2014*

| Lp. | Treść rekomendacji | Status realizacji | Wyniki weryfikacji wdrożenia rekomendacji |
|---|---|---|---|
| 2 | Tworzyć odrębne konta faktycznym użytkownikom komputerów. | Zrealizowano | Sprawdzono 4 komputery, na każdym z nich utworzone były odrębne konta pracowników korzystających z urządzenia. |
| 3 | Ograniczyć użytkownikom uprawnienia związane z możliwością samodzielnego instalowania oprogramowania (konta z ograniczeniami). | Zrealizowano | Na sprawdzonych 4 stanowiskach roboczych konta użytkowników posiadały ograniczenia. Stanowiska zarządzane były lokalnie. |
| 4 | Zapewnić wszystkim faktycznym użytkownikom komputerów imienne unikalne identyfikatory (loginy) oraz okresowo zmieniać hasła dostępu do komputerów i programów. | Zrealizowano | Zmiana haseł wymuszana jest przez informatyka – poprzez zmianę hasła na udostępnionych folderach na serwerze – powoduje to zmiany haseł przez użytkowników. |
| 5 | Zainstalować legalne oprogramowanie antywirusowe i zapewnić jego aktualność. | Zrealizowano | Na wszystkich testowanych 4 urządzeniach zainstalowane było aktualne oprogramowanie Kasperky antywirus ze zaktualizowaną bazą wirusów. |
| 6 | Na dowodach źródłowych dokumentujących zakupy sprzętu i oprogramowania umieszczać opisy ze wskazaniem numeru seryjnego i inwentarzowego właściwego komputera. | Zrealizowano | Nie było dokumentów zakupowych, dla komputerów otrzymanych jako darowizna z ZUS pozakładane były oddzielne teczki, w których wskazano numer inwentarzowy oraz numer seryjny (w przypadku gdy był na komputerze taki numer nadany). |
| 7 | Uzupełnić i na bieżąco aktualizować ewidencję funkcjonujących w DPS programów komputerowych. | Zrealizowano | Wprowadzono listę aplikacji, jaka może być zainstalowana na wszystkich stanowiskach roboczych oraz listę aplikacji dla stanowisk pracy (aplikacje dodatkowe m.in. księgowe, kadrowe, do wykonywania przelewów). |
| 8 | Przeanalizować regulacje wewnętrzne w zakresie BI i zmienić zapisy nieaktualne lub błędne. | Zrealizowano | Regulacje w zakresie BI zostały zaktualizowane oraz uszczegółowione w zakresie objętym audytem. |
| 9 | Z uzupełnionymi i zmienionymi regulacjami wewnętrznymi zapoznać wszystkich pracowników jednostki. Zapoznanie pracowników z regulacjami wewnętrznymi powinno być udokumentowane a potwierdzenia złożone do akt osobowych. | Zrealizowano | Odbyły się 2 spotkania pracowników w zakresie wprowadzenia zmian w procedurze BI. Zweryfikowano akta osobowe 5 pracowników – we wszystkich znajdowały się oświadczenia dotyczące zapoznania się regulacjami w zakresie BI oraz przetwarzania danych osobowych i związanej z tym odpowiedzialności. |

Audytorzy wewnętrzni:

Witold Przeszlakowski
Magdalena Pociecha