Stan cyberbezpieczeństwa Starostwa Powiatowego oraz jednostek powiatowych w kontekście wymogów dyrektywy NIS2.

Dyrektywa NIS2 – Directive (EU 2022/2555) to akt prawny Unii Europejskiej, który rozszerza obowiązki w zakresie cyberbezpieczeństwa na więcej podmiotów niż wcześniejsza Dyrektywa NIS1. Ma na celu podniesienie poziomu ochrony usług kluczowych i cyfrowych w UE. Dyrektywa weszła w życie 16 stycznia 2023 roku. Państwa członkowskie na implementację zapisów dyrektywy w przepisach krajowych miały do 17 października 2024 roku.

Polska pracuje nad projektem ustawy o zmianie Ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz niektórych innych ustaw (UC53), której celem jest transpozycja tej dyrektywy do polskiego porządku prawnego. Jednakże termin transpozycji minął, a proces legislacyjny w Polsce jeszcze się nie zakończył, podmioty objęte zakresem stosowania dyrektywy powinny rozpocząć przygotowania do spełnienia jej wymogów bez konieczności oczekiwania na wejście w życie nowej ustawy.

Starostwo Powiatowe w Oświęcimiu realizuje zadania publiczne w zakresie usług cyfrowych. Są to usługi geodezyjne świadczone przez dedykowany portal internetowy. Dodatkowo usługi WMS i WFS są wykorzystywane przez Geoportal Krajowy. Świadczone usługi wraz przetwarzanymi danymi, systemami teleinformatycznymi, bazy danych i zbiory danych osobowych muszą być odpowiednio chronione.

Pomimo, braku przepisów krajowych (Ustawa o Krajowym Systemie Cyberbezpieczenstwa) mających zaimplementować wymogi dyrektywy NIS2, Wydział Informatyki Starostwa Powiatowego w Oświęcimiu podjął już stosowne działania wdrażające zapisy dyrektywy NIS2.

Cyberbezpieczeństwo jest ciągłym i niekończącym się procesem, który z biegiem czasu misi być aktualizowany i udoskonalany. Z końcem roku 2023 został przeprowadzony przez firmę zewnętrzną audyt wewnętrzny bezpieczeństwa informacji i ochrony danych osobowych infrastruktury IT w oparciu o wymagania Krajowych Ram Interoperacyjności oraz zapisy normy PN ISO/IEC 27001 i UODO/RODO. Dodatkowo zinwentaryzowano zasoby IT i procesy (systemy, dane osobowe, dane wrażliwe, systemy komunikacji, kopie zapasowe), przejrzano również bieżące polityki i procedury bezpieczeństwa. Działania te pozwoliły na zdefiniowanie potrzeb i obszarów wymagających dostosowania do norm bezpieczeństwa.

W pierwszej kolejności w lutym 2024 roku wykonano projekt nowej sieci teleinformatycznej w budynku Starostwa Powiatowego w Oświęcimiu a w październiku 2024 roku wykonano prace instalatorskie nowego okablowania sieciowego na które otrzymano 25-letnią gwarancje producenta.

W listopadzie 2024 roku zostały zakupione urządzenia sieciowe spełniające wysokie standardy bezpieczeństwa. Urządzenia te pozwoliły na zakończenie przebudowy sieci teleinformatycznej w budynku starostwa. W tym samym miesiącu uruchomiono nową sieć monitoringu wizyjnego, który swym działaniem podnosi bezpieczeństwo fizyczne obiektu. Nowy system monitoringu pozwala m.in. na ciągłą kontrolę dostępu do serwerowni, w których umiejscowione są newralgiczne zasoby IT Starostwa.

W lipcu 2024 roku podpisano umowę w ramach projektu grantowego „Cyberbepieczny Samorząd” na dofinansowanie w kwocie 850.000 zł i wkładzie własnym 84.066 zł. Środki finansowe otrzymano jesienią 2024 roku. Wniosek projektowy został przygotowany z myślą o podniesieniu bezpieczeństwa IT Starostwa Powiatowego w Oświęcimiu jak i czterech jednostek podległych tj. Poradni Psychologiczno-Pedagogicznej w Oświęcimiu, Poradni Psychologiczno-Pedagogicznej w Kętach, Poradni Psychologiczno-Pedagogicznej w Brzeszczach i Młodzieżowym Domu Kultury w Oświęcimiu, które to Wydział Informatyki obsługuje w ramach swoich zadań.

Zadania w w/w projekcie, które będą realizowane w 2025 roku, pozwolą dostosować infrastrukturę IT starostwa i jednostek do wymagań dyrektywy NIS2 i nowoprojektowanej Ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Projekt zakłada zakup sprzętu, szkolenia dla pracowników i opracowanie dokumentacji z audytem końcowym. Zakup urządzeń UTM, serwerów, macierzy dyskowej, serwerów NAS, switchy, pozwoli na podniesienie bezpieczeństwa sieci teleinformatycznej i infrastruktury IT w starostwie i jednostkach. Sieć komputerowa będzie zarządzana i monitorowana w sposób ciągły dzięki zastosowaniu nowych rozwiązań systemowych za zakupionym sprzęcie. Nowe wydajniejsze harmonogramy kopii zapasowych na serwerach NAS i macierzy dyskowej pozwolą na podniesienie bezpieczeństwa gromadzonych i przetwarzanych danych.

Kolejnym elementem mającym na celu podniesienie bezpieczeństwa infrastruktury jest zakup zasilaczy awaryjnych UPS i agregatu prądotwórczego. Zapewnienie ciągłości działania systemów jest kluczowym elementem dla bezpieczeństwa infrastruktury a możliwe jest przy zachowaniu ciągłości zasilania. Nowy agregat prądotwórczy uniezależni instytucję od zdarzeń losowych lub celowych działań skutkujących brakiem dostaw energii elektrycznej. Zasilacze awaryjne UPS w jednostkach podległych pozwolą na podtrzymanie zasilania kluczowych urządzeń sieciowych.

Szkolenia pracowników i kadry zarządzającej są jednym z wymogów dyrektywy NIS2 i Ustawy o Krajowym Systemie Cyberbezpieczeństwa. W projekcie przewidziano przeszkolenie wszystkich pracowników starostwa i czterech jednostek podległych pod katem zwiększenia wiedzy w zakresie bezpieczeństwa IT. Dodatkowym cyklem szkoleń zostaną objęci pracownicy Wydziału Informatyki, który przejdą bardziej specjalistyczne szkolenia z tej dziedziny.

Temat szkoleń z dziedziny bezpieczeństwa IT nie jest tematem jednorazowym i zamkniętym. Pracownicy Starostwa w sposób ciągły mogą korzystać z materiałów szkoleniowych w tym zakresie. W przypadku pracowników Wydziału Informatyki jako Naczelnik kładę mocny nacisk na podnoszenie kompetencji pracowników przez udział w specjalistycznych szkoleniach. Co roku z powodzeniem składam wnioski aplikacyjne do Krajowego Funduszu Szkoleniowego na dofinansowanie szkoleń z tej dziedziny.

Zwieńczeniem realizowanego projektu będzie opracowanie dokumentacji w postaci Systemu Zarządzania Bezpieczeństwem Informacji w skład, którego wejdą nowe polityki bezpieczeństwa i procedury oparte na wdrożonych rozwiązaniach. Działaniem tym zostanie objęte nie tylko Starostwo lecz wszystkie trzy Poradnie Psychologiczno-Pedagogiczne i Młodzieżowy Dom Kultury. Całość projektu zakończy audyt.

Poza projektem sukcesywnie wymieniany jest sprzęt komputerowy i oprogramowanie na takie, które spełnia wysokie standardy bezpieczeństwa.

Wszystkie wymienione powyżej działania pozwolą na dostosowanie cyberbezpieczenstwa Starostwa Powiatowego w Oświęcimiu i czterech jednostek do wymogów NIS2 i UKSC. Jednak jak wcześniej wspomniałem nie jest to koniec działań w tym zakresie ponieważ bezpieczeństwo IT jest procesem, który w sposób ciągły musi być monitorowany i dostosowywany do zmieniającego się otoczenia.

Maciej Fudala

Naczelnik
Wydział Informatyki
(podpisano elektronicznie)