Czy na pewno jesteśmy bezpieczni?

Katarzyna Żółkiewska-Malicka

dyrektor ds. bezpieczeństwa informacji w ZETO sp. z o.o. w Lublinie. Audytor wewnętrzny, specjalista ds. bezpieczeństwa informacji z 20-letnim stażem pracy w zakresie przeprowadzania audytów cyberbezpieczeństwa, bezpieczeństwa informacji, ochrony danych osobowych oraz audytów śledczych. Auditor Wiodący systemu zarządzania bezpieczeństwem informacji wg ISO/IEC 27001. Członek Stowarzyszenia Praktyków Ochrony Danych Osobowych oraz Stowarzyszenia Inspektorów Ochrony Danych SABI. Ekspert w Cyber Women Community. Lider ISSA Polska Lublin. Członek CSO Council Społeczności Dyrektorów Bezpieczeństwa Informacji.

„Cyberbezpieczny Samorząd" to po „Cyfrowej Gminie" kolejny program, którego celem jest wzmocnienie krajowego systemu cyberbezpieczeństwa. Wnioski można składać do połowy grudnia 2024 r.

Projekt realizowany jest w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 „Cyberbezpieczny Samorząd" na podstawie ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027. Początkowo nabór wniosków trwać miał od 19.07.2023 r. do 30.09.2023 r., jednak z uwagi na to, że termin obejmował okres wakacyjny, wiele podmiotów publicznych obawiało się o jego dotrzymanie. Ostatecznie, po kilku jeszcze zmianach, termin składania wniosków został przesunięty na 14.12.2024 r.

Koszty niekwalifikowane w projekcie to wszelkie wydatki na zakup, dostawę lub usługi, które nie służą bezpośrednio wsparciu cyberbezpieczeństwa w JST. W szczególności są to:

a. komputery stacjonarne i przenośne;

b. urządzenia mobilne – smartfony lub tablety;

c. akcesoria i urządzenia peryferyjne, np. drukarki, skanery, urządzenia wielofunkcyjne, kserokopiarki, klawiatury, myszy;

d. materiały eksploatacyjne;

e. oprogramowanie biurowe, z wyłączeniem systemów operacyjnych niezbędnych do instalacji i utrzymania systemów bezpieczeństwa;

f. szkolenia informatyczne niezwiązane z cyberbezpieczeństwem, np. szkolenia z obsługi oprogramowania biurowego;

g. usługi dostępu do internetu, abonamenty telefoniczne.

Zakup przynajmniej części z tych urządzeń był możliwy w ramach „Cyfrowej Gminy". Osoby odpowiadające za IT w gminach podnosiły kwestię, że gdyby wiedziały o kolejnym projekcie skierowanym na SZBI (System Zarządzania Bezpieczeństwem Informacji), oprogramowanie np. typu EDR (*Endpoint Detection and Response*), XDR (*Extended Detection and Response*) czy oprogramowanie do wykonywania kopii zapasowych, to środki z „Cyfrowej Gminy" zostałyby przeznaczone na zakup sprzętu. Dałoby to możliwość dosprzętowienia urzędów i następnie zakupu dedykowanego oprogramowania.

Teoria sobie, praktyka …

Regulamin projektu kładzie duży nacisk na podnoszenie świadomości pracowników w zakresie cyberbezpieczeństwa. I jak to zwykle bywa, w teorii wszystko prezentuje się bardzo dobrze, a w praktyce wygląda zupełnie inaczej.

Ankieta dojrzałości cyberbezpieczeństwa już na starcie nastręczyła wielu problemów, gdyż niezbędne było określenie i opisanie stanu obecnego, stanu planowanego oraz opis planowanego zakresu zmian. Do tego doszła presja czasu z uwagi na okres wakacyjny, brak wcześniejszej zapowiedzi projektu oraz kilkukrotną zmianę terminu składania wniosków.

> *Informatyk w urzędzie musiał określić, co ma, co chce zakupić oraz jak wydatkowanie środków wpłynie na podniesienie poziomu cyberbezpieczeństwa w gminach.*

Nie wszystkie osoby odpowiadające w gminach za kwestie IT mają stosowną wiedzę w zakresie *cybersecurity* oraz rozwiązań dostępnych na rynku. Zainteresowani wskazują również, że z uwagi na nadal istniejące niedobory sprzętowe czy niewspierane systemy operacyjne, sam zakup oprogramowania nie zmieni istotnie sytuacji. Łatwo więc zidentyfikować pierwszą przeszkodę w osiągnięciu celu projektu – to niewystarczająca wiedza osób odpowiadających za kwestię IT w gminach w obszarze *security* oraz braki sprzętowe.

Podnoszenie poziomu świadomości pracowników jest kosztem kwalifikowanym i w ramach projektu można przeprowadzać szkolenia zarówno dla pracowników, jak i osób z IT. Najsłabszym ogniwem jest człowiek, na co również wskazują raporty powłamaniowe, bo atak najczęściej zaczyna się od pracownika. Wydawać by się więc mogło, że podmioty publiczne chętnie będą finansować szkolenia w ramach projektu.

Dla mnie ogromnym zaskoczeniem był opór osób z IT przed organizowaniem szkoleń dla pracowników. Najczęściej padał argument, że nie ma po co robić szkolenia, bo i tak nie będą wiedzieli, o co chodzi. Kilkakrotnie słyszałam szokujące dla mnie stwierdzenie, że szkolenie jest niepotrzebne, bo „my jesteśmy bezpieczni". W dzisiejszych czasach, gdy nie ma dnia bez informacji o kolejnej firmie, podmiocie publicznym czy koncernie, które padły ofiarą cyberprzestępców, takie stwierdzenie jest ryzykowne.

Panaceum jest banalnie wręcz proste. Wystarczy, żeby użytkownicy nie mieli możliwości instalowania oprogramowania na swoich stacjach roboczych, bo nie zainstalują przecież wtedy oprogramowania „złośliwego". Jeżeli takich argumentów używa osoba odpowiadająca za kwestie cyberbezpieczeństwa w dużym – jak na województwo lubelskie – urzędzie miasta, to jak podnosić ten poziom w podmiotach publicznych?

Praca u podstaw

Powinno się zacząć od podnoszenia wiedzy i kompetencji osób odpowiadających za kwestię IT, a dopiero później rozpoczynać realizację programów typu „Cyberbezpieczny Samorząd". Oczywiście, nie można wszystkich informatyków wrzucać do jednego worka, ale w mojej ocenie niewystarczający poziom wiedzy osób z IT ma negatywny wpływ na sposób realizacji projektu.

> *Może właściwym rozwiązaniem byłoby powołanie do życia podmiotu na wzór CUW (Centrum Usług Wspólnych), który z poziomu całego kraju badałby rzeczywisty stan bezpieczeństwa administracji publicznej, wypracowywałby minimalne standardy, jakie powinien w zakresie cyberbezpieczeństwa spełniać podmiot publiczny i byłby wsparciem przy realizacji projektów typu „Cyberbezpieczny Samorząd".*

Bardzo dużym problemem dla podmiotów publicznych jest finansowanie utrzymania – z własnych środków – oprogramowania np. typu NDR (*Network Detection and Response*) po zakończeniu projektu. Okres realizacji projektu grantowego wynosi maksymalnie 24 miesiące od dnia wejścia w życie Umowy o powierzenie Grantu, jednak nie później niż do 30.06.2026 r.

Oprogramowanie typu NDR zapewnia zespołom ds. bezpieczeństwa (w podmiotach publicznych będą to niekiedy pojedyncze osoby) wykrywanie i prognozowanie anomalii w ruchu sieciowym w czasie rzeczywistym. Pozwala na de-

tekcję zagrożeń, obsługę zdarzeń, monitorowanie sieci itp. Używanie tego typu oprogramowania to jednak luksus, bo oznacza koszt ok. 10 tys. zł. miesięcznie (to uśredniona wartość oferty przygotowanej dla średniej wielkości podmiotu zatrudniającego do 40 pracowników; są też oferty zdecydowanie wyższe). W trakcie trwania projektu urząd płaci za oprogramowanie z własnych środków. Pytanie, czy po 30.06.2026 r. jakiekolwiek urząd będzie stać na ponoszenie takich kosztów.

Są dwie strategie radzenia sobie z tym problemem. Jedna grupa podmiotów nie wpisywała we wnioskach tego typu rozwiązań, skupiając się na SZBI oraz szkoleniach. W zakresie sprzętowym decydowała się na zakup macierzy oraz dysków do macierzy, czyli elementów do wykonywania kopii zapasowych.

Druga grupa zdecydowała się na wpisanie we wniosku oprogramowania pozwalającego na wykrycie działań niepożądanych i ataków z pełną świadomością, że po zakończeniu trwałości projektu nie będą go utrzymywać z uwagi na koszty.

Problem w tym, że różnie wyglądają oceny wniosków pod kątem kwalifikowalności kosztów. Raz wyjmowane dyski do macierzy (do wykonania kopii bezpieczeństwa offline, deponowane w innej lokalizacji) są kwalifikowane jako koszt kwalifikowany, a raz nie. Opisywany przypadek dotyczy dwóch urzędów obsługiwanych przez tego samego informatyka, dlatego też opisy w obu wnioskach były identyczne.

W numerze 3/2023 „Domeny" podnosiłam kwestię nieprawidłowości czy wręcz anomalii w zakresie wykonywania audytów w ramach programu „Cyfrowa Gmina". Obawiam się, że i w tym projekcie będzie podobnie, bo wymagania co do podmiotów oraz osób wykonujących audyt się nie zmieniły.

Na pewno przeznaczanie środków na podnoszenie poziomu cyberbezpieczeństwa w podmiotach publicznych jest kierunkiem właściwym. Cieniem na realizacji tego projektu kładą się wskazane przeze mnie problemy: niewystarczająca wiedza w zakresie *cybersecurity* osób odpowiadających za IT w podmiotach publicznych, brak świadomości na temat zagrożeń, konieczność szkolenia pracowników oraz kwestie finansowe po zakończeniu trwania projektu. W celu uniknięcia takich problemów w przyszłości niezbędne jest przeprowadzanie przy takich projektach konsultacji z ekspertami, praktykami. Dobrym krokiem, który jako środowisko odbieramy pozytywnie, jest grudniowe zaproszenie nowego ministra cyfryzacji do udziału w branżowym spotkaniu. Trzymamy za słowo Pana Ministra, że będzie zasięgał opinii naszego środowiska przy planowaniu kolejnych projektów mających na celu zwiększenie cyfryzacji jednostek samorządu terytorialnego w obsarze zwiększenia poziomu cyberbezpieczeństwa.