Ministerstwo Cyfryzacji deklaruje kontynuację Cyberbezpiecznego Samorządu. Eksperci zwracają uwagę na bariery powstrzymujące potencjalnych beneficjentów przed udziałem.

Cyberbezpieczny Samorząd: wspierać by nie wrócić do poziomu zero

Aleksander Kostuch, inżynier Stormshieldu fot. mat prasowe imagopr

Wicepremier i minister cyfryzacji Krzysztof Gawkowski ogłosił kontynuację programu Cybebezpieczny Samorząd. Ekspert Stormshield wskazuje, że to dobra decyzja, bowiem niedostatek odpowiednich zasobów finansowych nadal stanowi istotną przeszkodę w budowie skutecznych strategii obronnych infrastruktury cybernetycznej. Dbałość o bezpieczeństwo IT JST istotna jest również w perspektywie implementacji wymogów dyrektywy NIS2.

Budżet kolejnej edycji programu nie został jeszcze ustalony. W obecnej edycji Cyberbezpiecznego Samorządu złożono wnioski na kwotę ok. 1,5 mld zł. Jednocześnie choć zainteresowanie pierwszą edycją programu było duże, to ponad 10% uprawnionych podmiotów do niego nie przystąpiło (wnioski złożyło 2 517 z 2 807 JST, z których zweryfikowano już ponad 2 tys.).

> *– Programy, takie jak Cyberbezpieczny Samorząd są krokiem w dobrą stronę. Bariera finansowa wciąż sprawia, że choć samorządy wiedzą o możliwych do nałożenia na nie karach, w przypadku niespełnienia nakładanych obowiązków co do zabezpieczenia swoich systemów IT, to nie zawsze mogą podjąć stosowne działania – komentuje Aleksander Kostuch, inżynier Stormshield, europejskiego wytwórcy rozwiązań z obszaru bezpieczeństwa IT. – Konsekwentne wsparcie zwiększa szanse uniknięcia scenariusza, gdy po upłynięciu ujętego w założeniach danego programu obligatoryjnego okresu realizacji zadań, samorządy z bezpieczeństwem wrócą do niskiego i nieakceptowanego poziomu – dodaje.*

Brak rozwiązań technicznych (np. firewalle następnej generacji, systemy ochrony stacji końcowych EDR), a także mechanizmów monitorowania i informowania o incydentach sprawia, że można stać się łatwym celem. Liczba ataków na JST w latach 2020-2022 zwiększyła się o 100 proc., a jak wskazują eksperci rok wyborczy sprzyja aktywności przestępców.

Środki dostępne w ramach programów rządowych pozwalają kompleksowo wzmocnić ochronę cyfrowej sfery funkcjonowania podmiotów samorządowych. Istotną w tym kontekście kwestią jest obowiązek utrzymania zakupionych rozwiązań, co dla niektórych beneficjentów może stanowić barierę.

Zgodnie z założeniem realizowanej obecnie edycji programu Cyberbezpieczny Samorząd, pozyskane środki mogą być przeznaczone na 2 lata utrzymania zakupionych rozwiązań, a dodatkowo beneficjenci muszą przez kolejne 2 lata sfinansować je z innych źródeł. Dla mniejszych samorządów może to być problemem, szczególnie gdy pojawia się konieczność zapewnienia ich z własnych funduszy. Przeszkodą może być także brak kwalifikowalności VAT. Przy maksymalnym dofinansowaniu 850 tys. złotych, oznacza to wydatek na poziomie niemal 200 tys. zł.

> *– Wójtom, burmistrzom czy starostom zwyczajnie łatwiej jest wydatkować ich ograniczone środki na coś namacalnego np. drogę, chodnik lub most. To z perspektywy niejednego wyborcy jest podstawą do oceny skuteczności i efektywności władz lokalnych, wyrażaną przy urnie wyborczej. Cyberbezpieczeństwo, w kontekście oceny funkcjonowania samorządu, znajduje się znacznie niżej w hierarchii ważności. Oczywiście nie jest to słuszne podejście, bo przecież gmina dysponuje olbrzymim katalogiem wrażliwych danych swoich mieszkańców, których kradzież może narazić ich*

> *na wiele problemów. Dlatego planując wydatki JST powinny położyć większy nacisk na inwestycje mające na celu podniesienie ogólnego poziomu własnego cyberbezpieczeństwa – podsumowuje Aleksander Kostuch, inżynier Stormshield.*

Dla cyberbezpieczeństwa samorządu ważna także dyrektywa NIS2

Ważnym aspektem w kontekście cyfrowej sfery funkcjonowania samorządów jest również zbliżające się wdrożenie do polskiego prawodawstwa założeń dyrektywy NIS2. Dyrektywa nakłada szereg obowiązków na podmioty kluczowe, wśród których znajdują się operatorzy infrastruktury krytycznej, m.in. raportowania incydentów, zarządzania ryzykiem i stosowania rozwiązań technicznych adekwatnych do jego poziomu. W ocenie eksperta, nawet 60 proc. podmiotów nie jest przygotowana na wymogi dyrektywy, nie mając wdrożonych odpowiednich rozwiązań w obszarze wykorzystywanych systemów przemysłowych. Dotyczy to w szczególności mniejszych operatorów infrastruktury krytycznej, z branż takich jak ciepłownictwo czy sieci wodociągowe.

> *– W Polsce jest niemal 2,5 tysiąca gmin, a w większości z nich działają lokalne przedsiębiorstwa wodociągowe czy ciepłownia. Te liczby unaoczniają skalę wyzwania. Uwagę zwraca brak podstawowej wiedzy na temat cyberbezpieczeństwa wśród zarządzających tymi podmiotami, którzy tę wiedzę powinny mieć, ponieważ z jednej strony osoba działająca w charakterze przedstawiciela prawnego danego przedsiębiorstwa będzie mogła być pociągnięta do odpowiedzialności za niewywiązanie się z obowiązku zapewnienia przestrzegania dyrektywy. Z drugiej, gdyż ewentualny „rachunek” za błędy czy niedopatrzenia zapłacą również*

> *mieszkańcy – mówi Piotr Zielaskiewicz z DAGMA Bezpieczeństwo IT i Stormshield.*

źródło informacji: imagopr