Bartłomiej Kocurek Kraków, 25 lutego 2026 r.

Radny Miasta Krakowa

Pan Aleksander Miszalski
Prezydent Miasta Krakowa
Urząd Miasta Krakowa
pl. Wszystkich Świętych 3-4
31-004 Kraków

Interpelacja Radnego Miasta Krakowa

na podstawie art. 24 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym

Szanowny Panie Prezydencie,

Działając w trybie interpelacji, w związku z obowiązkami wynikającymi z przepisów prawa krajowego oraz unijnego w zakresie cyberbezpieczeństwa, zwracam się o przedstawienie informacji dotyczących realizacji przez Miasto oraz podmioty zależne obowiązków określonych w szczególności w:
1. Ustawie o krajowym systemie cyberbezpieczeństwa (dalej: „UoKSC”),
2. Dyrektywie NIS2,
3. RODO.

I. Obowiązki wynikające z ustawy o krajowym systemie cyberbezpieczeństwa

Zgodnie z UoKSC operator usługi kluczowej jest zobowiązany do zapewnienia zarządzania bezpieczeństwem systemów informacyjnych wykorzystywanych do realizacji zadań publicznych.

Obowiązek ten obejmuje m.in.:
• wdrożenie odpowiednich i proporcjonalnych środków technicznych i organizacyjnych,

• obsługę incydentów bezpieczeństwa,
• zarządzanie ryzykiem,
• zapewnienie ciągłości działania systemów informacyjnych.

Dyrektywa NIS2 nakłada na podmioty kluczowe i ważne obowiązek regularnego przeprowadzania audytów bezpieczeństwa systemów informatycznych.

W związku z powyższym proszę o wskazanie:

1. Czy Miasto realizuje obowiązek zarządzania bezpieczeństwem systemów informacyjnych w oparciu o formalnie przyjętą politykę bezpieczeństwa?

2. Czy w okresie ostatnich 3 lat przeprowadzono audyty bezpieczeństwa systemów informacyjnych?

3. Czy którakolwiek ze spółek komunalnych została zakwalifikowana jako operator usługi kluczowej?

II. Zarządzanie ryzykiem i testowanie zabezpieczeń

Zgodnie z art. 32 ust. 1 RODO administrator danych jest zobowiązany wdrożyć dpowiednie środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa odpowiadający ryzyku, w tym m.in. regularne testowanie, mierzenie i ocenianie autecznośći środków technicznych i organizacyjnych.

W praktyce oznacza to obowiązek okresowych testów bezpieczeństwa, w tym testów penetracyjnych i audytów.

W związku z powyższym proszę o odpowiedź:

1. Czy w okresie ostatnich 3 lat przeprowadzano testy penetracyjne systemów i portali miejskich? Jeśli tak to jakich i kiedy?

2. Czy prowadzony jest formalny proces zarządzania podatnościami?

3. Ile podatności zidentyfikowano w ostatnich 3 latach – z podziałem na klasyfikację według severity CVSS v3.1?

4. Jaki był średni oraz maksymalny czas usunięcia podatności sklasyfikowanych jako High i Critical?

5. Ile podatności pozostaje nieusuniętych na dzień udzielenia odpowiedzi?

III. Przygotowanie do wdrożenia Dyrektywy NIS2

Dyrektywa NIS2 znacząco rozszerza obowiązki podmiotów publicznych i komunalnych, w szczególności w zakresie stosowania środków obejmujących testowanie i ocenę skuteczności zabezpieczeń.

W związku z trwającym procesem implementacji dyrektywy proszę o wskazanie:

1. Czy przeprowadzono analizę zgodności (gap analysis) z wymogami NIS2?

2. Czy opracowano plan dostosowawczy obejmujący Miasto oraz spółki komunalne?

3. Czy Władze Miasta zostały formalnie poinformowane o potencjalnej osobistej odpowiedzialności wynikającej z NIS2?

4. Czy przeprowadzono analizę ryzyka w kontekście nowych obowiązków regulacyjnych?

IV. Procedura ujawniania podatności

Program bug bounty jest sformalizowanym mechanizmem współpracy pomiędzy właścicielem systemów teleinformatycznych a niezależnymi badaczami bezpieczeństwa, polegającym na umożliwieniu legalnego testowania określonych zasobów cyfrowych oraz zgłaszania wykrytych podatności w zamian za wynagrodzenie lub inną formę uznania. Jego istotą jest stworzenie kontrolowanego i zgodnego z prawem kanału ujawniania luk bezpieczeństwa, zanim zostaną one wykorzystane w sposób nieuprawniony. Program taki może funkcjonować w oparciu o jasno określony zakres testów (scope), zasady odpowiedzialnego ujawniania podatności (responsible disclosure), procedurę ich weryfikacji oraz mechanizm klasyfikacji – najczęściej według standardu CVSS. W sektorze publicznym bug bounty może stanowić uzupełnienie audytów bezpieczeństwa i testów penetracyjnych, wpisując się w obowiązek regularnego testowania skuteczności środków technicznych i organizacyjnych, o którym mowa w przepisach prawa dotyczących cyberbezpieczeństwa.

Jednym z pierwszych europejskich samorządów, które zdecydowały się na wdrożenie takiego rozwiązania, było miasto Wiedeń. Program został uruchomiony przez administrację miejską jako element szerszej strategii cyfrowej miasta i działań na rzecz zwiększenia odporności infrastruktury teleinformatycznej. Wdrożenie poprzedziła analiza prawna i organizacyjna, obejmująca ocenę ryzyk związanych z odpowiedzialnością karną i cywilną, przygotowanie zasad tzw. safe harbour, czyli ochrony badaczy działających w granicach regulaminu, a także określenie wewnętrznych procedur obsługi zgłoszeń.

Miasto opublikowało oficjalny regulamin programu, w którym zdefiniowano zakres systemów objętych testowaniem, dopuszczalne metody działania, zasady komunikacji z zespołem bezpieczeństwa oraz sposób klasyfikowania i raportowania podatności.

Program wiedeński ma charakter klasycznego bug bounty – przewiduje wypłatę nagród finansowych uzależnionych od wagi i wpływu wykrytej podatności na poufność, integralność i dostępność systemów miejskich. Klasyfikacja luk odbywa się w oparciu o standardowe metody oceny ryzyka, a wynagrodzenie przyznawane jest po potwierdzeniu podatności i jej usunięciu. Jednocześnie miasto zapewniło badaczom formalny, bezpieczny kanał komunikacji oraz gwarancję, że działania prowadzone zgodnie z regulaminem nie będą skutkować odpowiedzialnością prawną.

Wdrożenie programu nie zastąpiło audytów bezpieczeństwa ani testów penetracyjnych realizowanych przez podmioty zewnętrzne, lecz zostało zaprojektowane jako ich stałe uzupełnienie. Model ten opiera się na założeniu ciągłego, rozproszonego testowania systemów publicznych przez społeczność ekspertów, co pozwala skrócić czas wykrywania podatności oraz zwiększyć transparentność działań administracji w obszarze cyberbezpieczeństwa. W efekcie program stał się elementem systemowego podejścia do zarządzania ryzykiem, wzmacniając odporność cyfrową miasta oraz budując partnerskie relacje z międzynarodowym środowiskiem badaczy bezpieczeństwa.

W świetle obowiązku zapewnienia odpowiednich środków bezpieczeństwa oraz testowania ich skuteczności, proszę o informację:

1. Czy w Mieście funkcjonuje formalna procedura zgłaszania podatności (coordinated/responsible disclosure)?

2. Czy istnieje dedykowany kanał zgłaszania podatności przez niezależnych badaczy bezpieczeństwa?

3. Czy analizowano możliwość wdrożenia programu typu bug bounty jako elementu systemowego zarządzania ryzykiem?

4. Czy w ciągu ostatnich 3 lat, niezależni badacze zgłaszali nieprawidłowości systemów miejskich lub spółek miejskich?

Dyrektywa NIS2 istotnie podnosi standard należytej staranności wymaganej od kierownictwa jednostek publicznych. W związku z powyższym uprzejmie proszę o szczegółową odpowiedź zawierającą dane liczbowe, wskazanie podstaw organizacyjnych realizacji obowiązków ustawowych oraz informację o planowanych działaniach dostosowawczych.

Z poważaniem,
Bartłomiej Kocurek