Sekretarz Miasta Szczecin
Ryszard Słoka
pl. Armii Krajowej 1, 70-456 Szczecin
tel. +4891 42 45 200, fax +4891 42 22 340
rsloka@um.szczecin.pl * www.szczecin.eu

Szczecin, 26.09.2025 rok

Pan Stanisław Kaup

Radny Miasta Szczecin

W odpowiedzi na interpelację numer 1526 z dnia 17 września 2025 roku dot. zapewnienia bezpieczeństwa informacji i ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego, przekazuję odpowiedzi na zamieszczone pytania:

1. Jak miasto Szczecin zapewnia bezpieczeństwo danych osobowych i innych istotnych informacji przetwarzanych w urzędach?

   Realizacja zabezpieczenia danych osobowych w realiach pracy Urzędu Miasta Szczecin realizowane jest w wielu kierunkach, zabezpieczenia techniczne, proceduralne oraz organizacyjne i osobowe.

   Zabezpieczenia techniczne obejmują: regularne inwestycje w rozwiązania sprzętowe zwiększające bezpieczeństwo danych – zaawansowane zapory sieciowe, przestrzeń dyskową odporną na mechanizmy ransomware, nowoczesne urządzenia sieciowe, nowej generacji zintegrowane systemy detekcji i przeciwdziałania, służące do kompleksowej ochrony przed zagrożeniami cybernetycznymi, w dniu 02.06.2025 podpisano umowę z jednym z liderów rozwiązań na rynku polskim w zakresie ochrony przed cyberzagrożeniami na usługę SOC i SIEM , SIEM (Security Information and Event Management) to system informatyczny zbierający, analizujący i korelujący dane bezpieczeństwa z różnych źródeł, dla wykrywania incydentów i generowania alertów. SOC (Security Operations Center) to zespół specjalistów, którzy korzystają z narzędzi takich jak SIEM do ciągłego monitorowania, wykrywania, analizowania i reagowania na zagrożenia cybernetyczne w organizacji, zapewniając jej bezpieczeństwo.

   Zabezpieczenia proceduralne (zabezpieczenia wynikające m.in. z dyrektywy NIS2, ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI)) : procesy oceny i zarządzania ryzykiem dla systemów IT, zarządzanie incydentami – posiadanie procedur wykrywania, reagowania i dokumentowania incydentów cyberbezpieczeństwa, zgłaszanie incydentów – obowiązek zgłaszania poważnych incydentów do właściwego CSIRT (CSIRT NASK). UM Szczecin jest użytkownikiem systemu S46 – jest to zintegrowany system teleinformatyczny wspierający cyberbezpieczeństwo w Polsce, którego głównym celem jest ułatwienie zgłaszania i obsługi incydentów, wymiana informacji o zagrożeniach oraz współpraca między uczestnikami Krajowego Systemu Cyberbezpieczeństwa (KSC), takimi jak operatorzy usług kluczowych czy jednostki administracji, kontrola bezpieczeństwa dostawców i usługodawców, współpraca z innymi instytucjami państwowymi przy poważnych incydentach, audyt i testy, prowadzenie i utrzymywanie polityk, procedur oraz dowodów ich realizacji (np. rejestry incydentów).

   Zabezpieczenia organizacyjne i osobowe: audyt i testy (pentesty), przeglądy bezpieczeństwa i przegląd zgodności, szkolenia pracowników, podnoszenie świadomości w zakresie cyberbezpieczeństwa wśród urzędników - szkolenia w zakresie określonych zagadnień, wewnętrzna platforma e-learningowa,

ustanowiony System Zarządzania Bezpieczeństwem Informacji i Polityka Bezpieczeństwa Informacji, zasady zarządzania dostępem (zasada minimalnych uprawnień, role i poziomy dostępu), segregacja kont (administracyjne/użytkownika), w lutym 2024 roku został powołany specjalista ds. cyberbezpieczeństwa, egzekwowana jest dyscyplina w zakresie przestrzegania procedur (np. polityki haseł, certyfikatów, zgłaszania incydentów).

2. Czy zostały wprowadzone procedury identyfikacji zbiorów danych wymagających ochrony, w tym danych niebędących danymi osobowymi?
Tak, prowadzony jest systematyczny przegląd wszystkich komórek organizacyjnych i systemów, w których mogą być przetwarzane dane osobowe, oraz formalnym wyodrębnieniu i opisaniu zbiorów danych zgodnie z kryteriami prawnymi i operacyjnymi.

3. Czy miasto posiada wdrożony System Zarządzania Bezpieczeństwem Informacji (SZBI)? Jeśli tak, to czy regularnie przeprowadzane są przeglądy jego skuteczności, zgodnie z przepisami rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności?
Tak. Prowadzone są przeglądy dostosowujące do pojawiających się zagrożeń cyberbezpieczeństwa.

4. Czy w urzędach miejskich zostały opracowane plany ciągłości działania i plany odtworzeniowe? Jeśli tak, czy zostały one testowane, aby zapewnić ich skuteczność w przypadku awarii systemów informatycznych?
Nie, w rozumieniu normy ISO 22301, tak w zakresie przynależnym Wydziałowi Zarządzania Kryzysowego i Ochrony Ludności oraz wynikające z dobrej praktyki i rutynowych działań Wydziału Informatyki.

5. Jakie zabezpieczenia zostały wprowadzone w serwerowniach miejskich, aby zapobiec zagrożeniom zewnętrznym, takim jak pożar czy zalanie?
Czujnik temperatury, czujnik dymu z automatycznym raportowaniem stanu, podniesiona przeciwzalewowa podłoga, drzwi ogniotrwałe, przekonstruowany układ hydrauliki w kondygnacjach powyżej serwerowni, monitoring wizyjny,

6. Czy pracownicy odpowiedzialni za przetwarzanie danych w urzędach są regularnie szkoleni w zakresie bezpieczeństwa informacji? Jeśli nie, czy miasto planuje wprowadzenie obowiązkowych szkoleń z tego zakresu?
Tak.

7. Jak miasto zapewnia bezpieczeństwo informacji w kontekście współpracy z zewnętrznymi dostawcami usług IT? Czy wszystkie umowy z takimi dostawcami zawierają odpowiednie zapisy gwarantujące poufność przetwarzanych danych?
Poprzez zawarcie Umowy Powierzenia Przetwarzania Danych Osobowych.
Tak umowy zawierają odpowiednie zapisy gwarantujące poufność przetwarzanych danych.

8. W jaki sposób miasto monitoruje i testuje kopie zapasowe danych? Czy przechowywane są one poza miejscem wytworzenia, zgodnie z najlepszymi praktykami w zakresie bezpieczeństwa informacji?
Wydział Informatyki sukcesywnie odtwarza dane z kopii zapasowych. Fizycznie kopie są przechowywane w trzech różnych lokalizacjach.
W ramach ostatniego cyklu projektu „Cyberbezpieczny Samorząd" zakupiono i wdrożono wydajne, skalowalne repozytorium kopii zapasowych. Jest to system zaprojektowany z myślą o ochronie przed

ransomware, szybkim odzyskiwaniu danych oraz ekonomicznym wykorzystaniu przestrzeni dyskowej poprzez deduplikację.

9. Czy w urzędach miejskich przeprowadzane są coroczne audyty wewnętrzne z zakresu bezpieczeństwa informacji? Jeśli tak, jakie działania zostały podjęte w wyniku przeprowadzonych audytów?
   Tak.
   Każdorazowo wyniki audytu są podstawą dla doskonalenia stosowanych rozwiązań i procedur w organizacji.

10. Czy miasto planuje zwiększenie wsparcia dla jednostek samorządu terytorialnego w zakresie wdrażania rozwiązań dotyczących bezpieczeństwa informacji, w oparciu o rekomendacje zawarte w raporcie NIK?
    Urząd Miasta Szczecin współpracuje z wieloma jednostkami w zakresie cyberbezpieczeństwa.