Zarządzenie nr 72/2020
Burmistrza Miasta Radymna
z dnia 26 lipca 2020 r.

w sprawie wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz wprowadzenia instrukcji zarzadzania zdarzeniami, mającymi negatywny wpływ na cyberbezpieczeństwo (tzw. incydentami).

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2020 r., poz. 713 ze zmianami) w zw. z art. 21 ust 1 i 3 oraz ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2018.1560),

zarządzam co następuje:

§ 1. Urząd Miasta Radymna (dalej: Podmiot Publiczny) realizując zadania publiczne, które są zależne od systemu informatycznego:

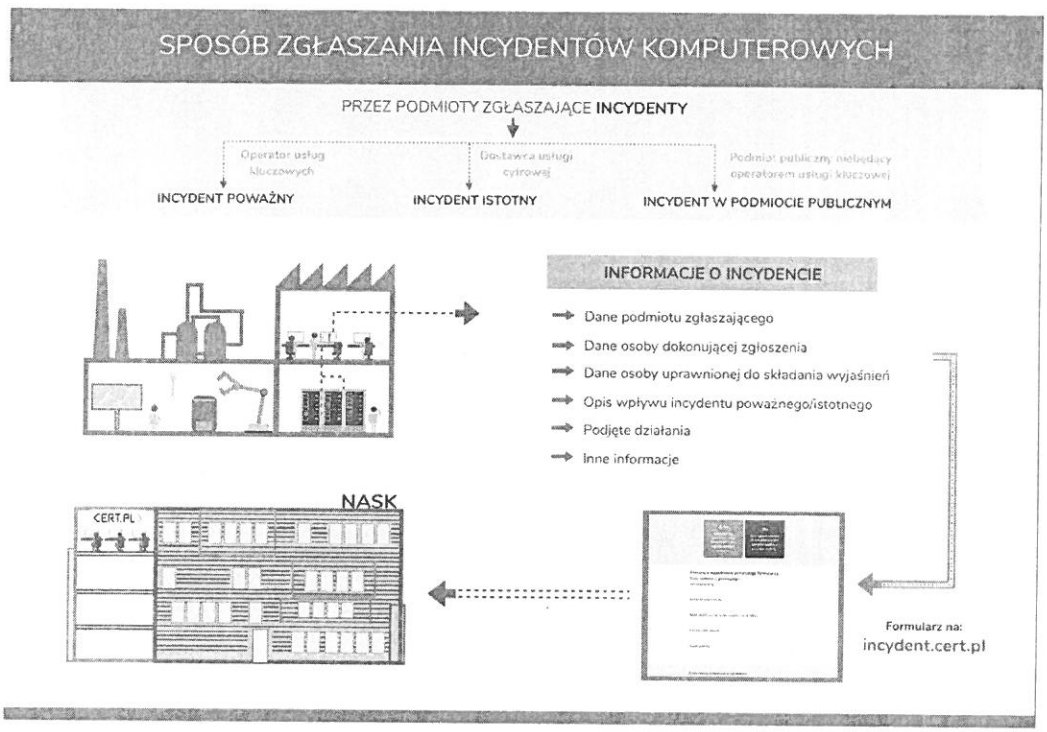
a. zapewnia zarządzanie incydentem w Podmiocie Publicznym – zasady zarządzania zostały określone w załączniku numer 1 do niniejszego zarządzenia;
b. zgłasza incydent w Podmiocie Publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;
c. zapewnia obsługę incydentu w Podmiocie Publicznym we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;
d. zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej.

§2. 1. Na osobę odpowiedzialną za utrzymywanie kontaktów w Podmiocie Publicznym z podmiotami krajowego systemu cyberbezpieczeństwa wyznacza się Pana Daniela Fijałkowskiego.

2. Ww. osoba jest zobowiązana dokonać swojej rejestracji w terminie 14 od wejścia w życie niniejszego zarządzenia wypełniając formularz na stronie: https://incydent.cert.pl/osoba-kontaktowa.
3. Ww. osoba jest zobowiązana poinformować Kierownika Podmiotu Publicznego o potwierdzeniu otrzymania formularza rejestracyjnego przez CSIRT NASK.

§ 3.1. Incydenty objęte obowiązkiem zgłaszania:

a. Incydent w podmiocie publicznym to incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego;
b. Ze względu na skalę, charakter i rodzaj działalności Podmiotu Publicznego incydenty dotyczące dostawców usług cyfrowych (incydent istotny) oraz operatorów usług kluczowych (Incydent poważny) nie znajdują zastosowania.
c. Ścieżka zgłaszania incydentów w Podmiocie Publicznym

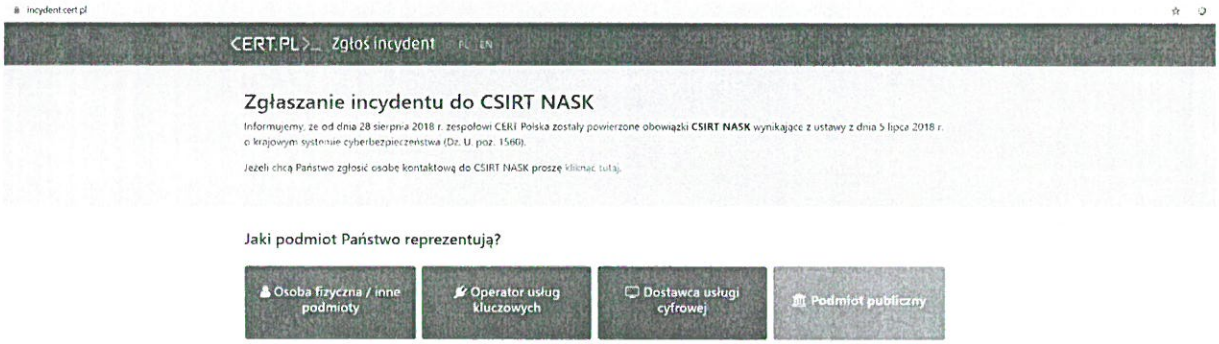


§ 4. 1. Osoba odpowiedzialną za utrzymywanie kontaktów w Podmiocie Publicznym z podmiotami krajowego systemu cyberbezpieczeństwa w momencie powzięcia informacji o zaistnieniu lub podejrzeniu incydentu niezwłocznie dokumentuje je w formularzu zgłoszenia incydentu bezpieczeństwa cybernetycznego, który stanowi załącznik numer 2 do niniejszego zarządzenia. Formularz jest dokumentem który pozostaje w Podmiocie Publicznym dla celów dowodowych.

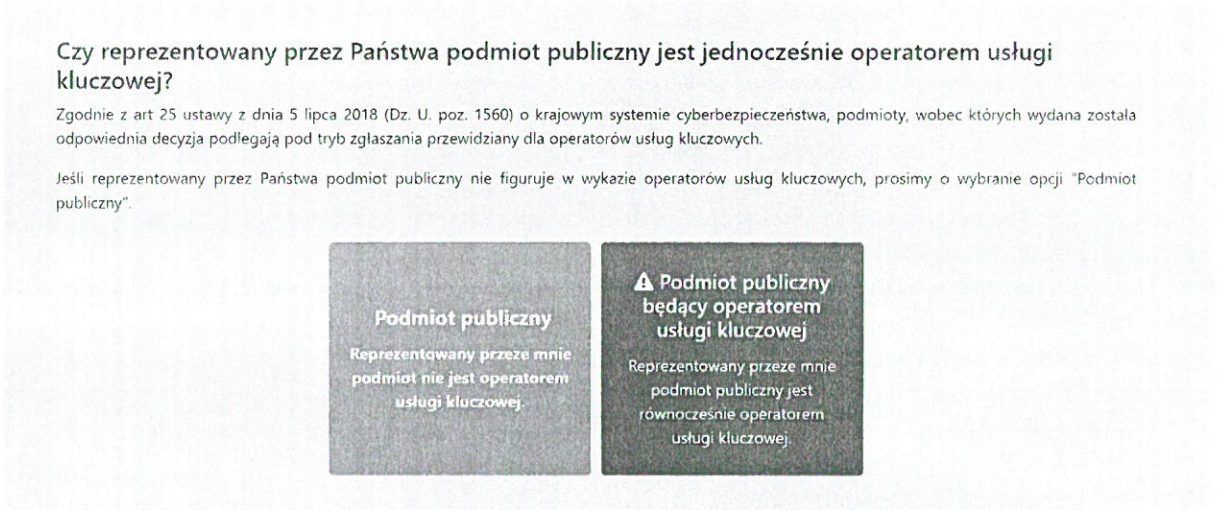
2. Zgłoszenie incydentu do CSIRT NASK na podstawie art. 24 ustawy przekazywane są w postaci elektronicznej poprzez formularz dostępny na stronie www.incydent.cert.pl. Jedynie w przypadku braku możliwości przekazania zgłoszenia w postaci elektronicznej, przesyła się je przy użyciu innych dostępnych środków komunikacji.

§ 5. Szczegółowa instrukcja zgłoszenia.

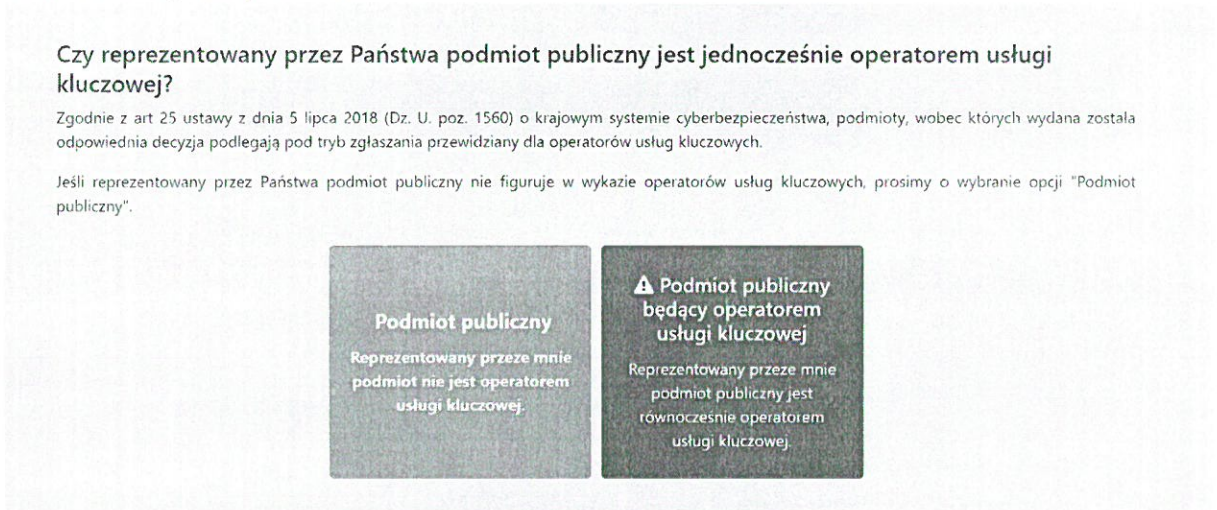
a. Krok pierwszy – wybierz pole „Podmiot Publiczny";



b. Krok drugi – wybierz pole „Podmiot Publiczny";



c. Krok trzeci – wybierz pole „Tak";



d. Krok czwarty – w formularzu wprowadź dane jakie zostały zebrane w Formularzu zgłoszenia incydentu bezpieczeństwa cybernetycznego, który stanowi załącznik numer 2 do niniejszego zarządzenia.

e. Krok piąty – uzupełnienie formularza „CAPTCHA" oraz wysłanie zgłoszenia.

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

Pieczątki i podpis

BURMISTRZ

Mieczysław Piziurny

Załącznik numer 1 do Zarządzenia numer 72/2020

Ogólne zasady postępowania

1. Raportowanie: Naruszenia dotyczące systemów informatycznych.
   1.1. Każda osoba zatrudniona w Podmiocie Publicznym, która stwierdzi lub podejrzewa wystąpienie incydenty cyberbezpieczeństwa, niezwłocznie informuje o tym fakcie osobę odpowiedzialną za utrzymywanie kontaktów (dalej osoba kontaktowa) w Podmiocie Publicznym z podmiotami krajowego systemu cyberbezpieczeństwa.
   1.2. Osoba kontaktowa podejmuje działania zmierzające do ustalenia okoliczności incydentu dokumentując je w formularzu stanowiącym załącznik numer 2 do niniejszej instrukcji.
   1.3. Informacja o podejrzeniu wystąpieniu incydentu cyberbezpieczeństwa jest niezwłocznie przekazywana przez osobą kontaktową do CSIRT NASK.
   1.4. Osoba kontaktowa podejmuje odpowiednie kroki opisane w „Procedurze postępowania dla incydentów cyberbezpieczeństwa" (poniżej) lub realizuje instrukcje / wytyczne otrzymane od CSIRT NASK.

Procedura postępowania dla incydentów cyberbezpieczeństwa

1. W przypadku stwierdzenia incydentu cyberbezpieczeństwa w systemie informatycznym osoba kontaktowa podejmuje następujące działania:
   1.1. fizycznie odłączyć urządzenia i segmenty sieci, które mogły umożliwić dostęp do bazy danych osobie nieupoważnionej,
   1.2. zapisać wszelkie informacje związane z danym zdarzeniem, a szczególnie: dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych lub czas samodzielnego wykrycia tego faktu,
   1.3. na bieżąco wygenerować i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem,
   1.4. przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali szkód i sposobu dostępu do danych osoby niepowołanej.
2. Następnie osoba kontaktowa prowadzi działania zmierzające do zminimalizowania szkód i zabezpieczenia śladów naruszenia. Osoba kontaktowa przestępuje do zabezpieczenia systemu w szczególności przez:
   2.1. wylogowanie użytkownika podejrzanego o naruszenie ochrony danych osobowych,
   2.2. zmianę hasła na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.
3. Po wyeliminowaniu bezpośredniego zagrożenia Osoba Kontaktowa przeprowadzi wstępną analizę stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych w systemie, która obejmuje sprawdzenie:
   3.1. stanu urządzeń wykorzystywanych do przetwarzania danych osobowych,
   3.2. zawartości zbioru danych osobowych,
   3.3. sposobu działania programu,
   3.4. jakości komunikacji w sieci teleinformatycznej,
   3.5. możliwości obecności wirusów komputerowych.
4. Po analizie wstępnej Osoba kontaktowa przeprowadza szczegółową analizę stanu systemu informatycznego obejmującą identyfikację:
   4.1. rodzaju zaistniałego zdarzenia,
   4.2. sposobu dostępu do danych osoby nie upoważnionej,
   4.3. ewentualnych szkód lub zniszczeń,
   4.4. wszelkich potencjalnych skutków dla osób oraz rekomendowanych środków naprawczych.
5. Po dokonaniu szczegółowej analizy Osoba Kontaktowa przywraca normalne działanie systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, niezbędne jest odtworzenie jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego umożliwienia dostępu tą samą drogą osobie niepowołanej.
6. Po przywróceniu prawidłowego stanu systemu Osoba Kontaktowa określa przyczyny naruszenia ochrony danych osobowych oraz podejmuje kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości, uwzględniając poniższe przypadki:
   6.1. jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych w systemie informatycznym należy przeprowadzić dodatkowe szkolenie a pozostałych pracowników poinformować o okolicznościach błędu,
   6.2. jeżeli przyczyną zdarzenia było uaktywnienie złośliwego oprogramowania, należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe,
   6.3. jeżeli przyczyną zdarzenia było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, przeprowadza się dla niej dodatkowe szkolenie z zasad bezpieczeństwa i prawidłowej pracy w systemach,
   6.4. jeżeli przyczyną zdarzenia było włamanie w celu pozyskania bazy danych osobowych, należy przeanalizować wdrożone środki zabezpieczające, w celu zapewnienia skuteczniejszej ochrony systemów,
   6.5. jeżeli przyczyną zdarzenia był zły stan urządzenia lub sposób działania programu, należy niezwłocznie przeprowadzić czynności kontrolne lub serwisowe.
7. Jeżeli incydent cyberbezpieczeństwa wpływa na osoby, których dane osobowe są przetwarzane przez Podmiot Publiczny, równolegle do działań opisanych w niniejszej Instrukcji stosuje się procedury właściwe dla naruszeń bezpieczeństwa danych osobowych określonych odrębnym zarządzeniem kierownika Podmiotu Publicznego.

Formularz zgłoszenia incydentu bezpieczeństwa cybernetycznego	
Dane podmiotu zgłaszającego	
Pełna nazwa firmy	
Numer REGON/NIP/KRS	
Adres siedziby (ulica, numer budynku, numer lokalu)	
Kod pocztowy siedziby	
Miasto siedziby	
Dane osoby dokonującej zgłoszenia	
Imię i nazwisko osoby zgłaszającej	
Numer telefonu osoby zgłaszającej	
Adres e-mail osoby zgłaszającej	
Dane osoby uprawnionej do składania wyjaśnień	
Imię i nazwisko osoby do kontaktu w sprawie	
Numer telefonu osoby do kontaktu w sprawie	
Adres e-mail osoby do kontaktu w sprawie	
Opis wpływu incydentu w podmiocie publicznym *Wypełnij poniższy formularz zgodnie z wiedzą, którą posiadasz w chwili zgłoszenia. Istotne aktualizacje będziesz mógł wysłać później przez pocztę elektroniczną. Wystarczy, że podasz numer zgłoszenia, który nadamy po otrzymaniu tego formularza.* *Pamiętaj, aby wysyłając zgłoszenie oznaczyć informacje prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa. Aby to zrobić, użyj nawiasów kwadratowych, na przykład: [Incydent w systemie bankowym miał wpływ na 10 tysięcy użytkowników końcowych.]* *Uwaga: Nieuzasadnione użycie oznaczeń może wydłużyć czas odpowiedniej reakcji.*	
Czy incydent miał wpływ na realizację zadań publicznych? Jeśli tak, na jakie?	
Czy możesz określić dokładną lub przybliżoną liczbę osób, na które ma wpływ incydent?	
Czy znasz dokładny lub przybliżony czas wystąpienia oraz wykrycia incydentu?	
Czy możesz geograficznie określić obszar, którego dotyczy incydent?	
Czy ustaliłeś przyczynę incydentu?	
Czy ustaliłeś skutki oddziaływania incydentu na twoje systemy informacyjne?	
Opisz najdokładniej jak potrafisz przebieg incydentu	
Podjęte działania	
Czy podjęto działania zapobiegawcze w związku z incydentem? Jeśli tak, prosimy opisać te działania.	
Jakie działania naprawcze podjąłeś w związku z incydentem?	
Inne informacje	
Inne istotne informacje	
Załączniki	
Podpisy i data	