Zarządzenie Nr 29/22
Wójta Gminy Grodzisko Dolne
z dnia 26 maja 2022

w sprawie wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa i ustalenia procedury zgłaszania incydentów

Na podstawie art. 30 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz.U. z 2022r. poz. 559), oraz art. 21 ust 1 i 3 oraz ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2022, poz. 1369 z późn. zm.)

Wójt Gminy Grodzisko Dolne
zarządza co następuje:

§ 1

Urząd Gminy Grodzisko Dolne realizując zadania publiczne, które są zależne od systemu informatycznego:

1) zapewnia zarządzanie incydentem. Zasady zarządzania zostały określone w załączniku Nr 1 do niniejszego zarządzenia;
2) zgłasza incydent niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;
3) zapewnia obsługę incydentu we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;
4) 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.

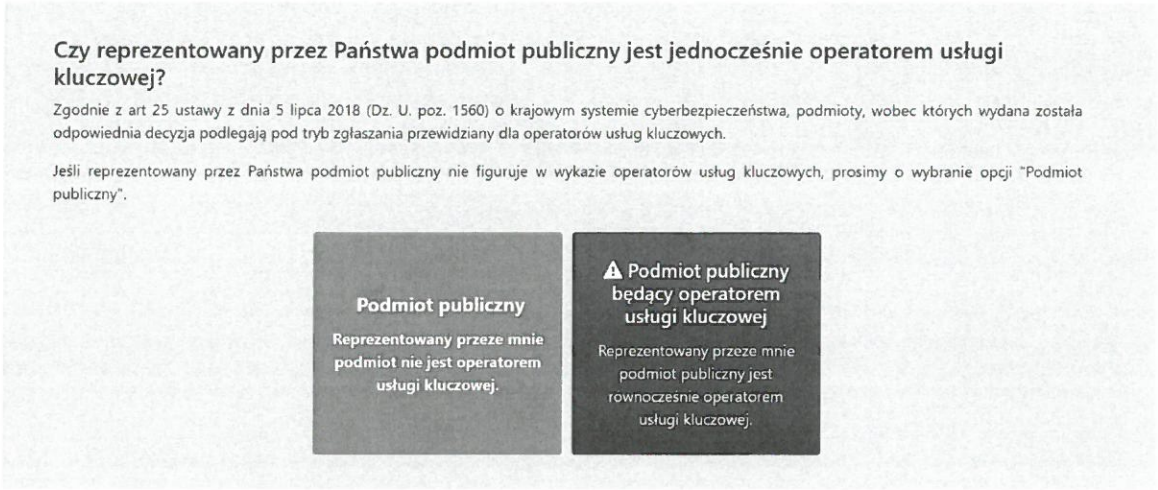
§ 2

1. Na osobę odpowiedzialną za utrzymywanie kontaktów w Urzędzie Gminy Grodzisko Dolne z podmiotami krajowego systemu cyberbezpieczeństwa wyznacza się Pana Krzysztofa Laskowskiego, nr tel: 17-242 82 65; mail: informatyk@grodziskodolne.pl. 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.
2. Ww. osoba jest zobowiązana poinformować Sekretarz Gminy Grodzisko Dolne o potwierdzeniu otrzymania formularza rejestracyjnego przez CSIRT NASK.

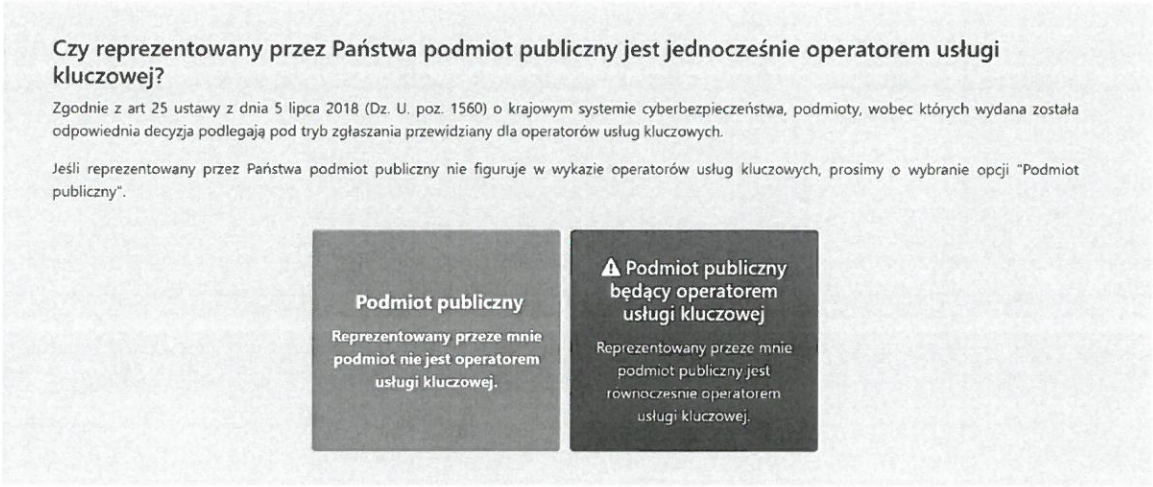
§ 3

1. Incydenty objęte obowiązkiem zgłaszania to incydenty, które powodują lub mogą spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego;
2. Ze względu na skalę, charakter i rodzaj działalności Urzędu Gminy incydenty dotyczące dostawców usług cyfrowych (incydent istotny) oraz operatorów usług kluczowych (incydent poważny) nie znajdują zastosowania.
3. Ścieżka zgłaszania incydentów:

2) Krok drugi – wybierz pole „Podmiot Publiczny”;



3) Krok trzeci – wybierz pole „Tak”;



4) Krok czwarty – w formularzu wprowadź dane, jakie zostały zebrane w Formularzu zgłoszenia incydentu bezpieczeństwa cybernetycznego, który stanowi załącznik Nr 2 do niniejszego zarządzenia.
5) Krok piąty – uzupełnienie formularza „CAPTCHA” oraz wysłanie zgłoszenia.

§ 6

1. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
mgr Jacek Chmura

Załącznik Nr 1 do Zarządzenia Nr 29/22
Wójta Gminy Grodzisko Dolne

OGÓLNE ZASADY POSTĘPOWANIA

§ 1

1. Raportowanie: Naruszenia dotyczące systemów informatycznych.
   1) Każda osoba zatrudniona w Urzędzie Gminy Grodzisko Dolne, która stwierdzi lub podejrzewa wystąpienie incydentu cyberbezpieczeństwa, niezwłocznie informuje o tym fakcie osobę odpowiedzialną za utrzymywanie kontaktów (dalej osoba kontaktowa) z podmiotami krajowego systemu cyberbezpieczeństwa.
   2) Osoba kontaktowa podejmuje działania zmierzające do ustalenia okoliczności incydentu dokumentując je w formularzu stanowiącym załącznik Nr 2 do niniejszej instrukcji.
   3) Informacja o podejrzeniu wystąpieniu incydentu cyberbezpieczeństwa jest niezwłocznie przekazywana przez osobą kontaktową do CSIRT NASK.
   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

§ 2

1. W przypadku stwierdzenia incydentu cyberbezpieczeństwa w systemie informatycznym osoba kontaktowa podejmuje następujące działania:
   1) fizycznie odłącza urządzenia i segmenty sieci, które mogły umożliwić dostęp do bazy danych osobie nieupoważnionej,
   2) zapisuje wszelkie informacje związane z danym zdarzeniem, a szczególnie: dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych lub czas samodzielnego wykrycia tego faktu,
   3) na bieżąco wygeneruje i wydrukuje (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzy je datą i podpisem,
   4) przystąpi 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:
   1) wylogowanie użytkownika podejrzanego o naruszenie ochrony danych osobowych,
   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:
   1) stanu urządzeń wykorzystywanych do przetwarzania danych osobowych,

Załącznik Nr 2 do Zarządzenia Nr 29/22
Wójta Gminy Grodzisko Dolne

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 rozliczeń miał wpływ na wszystkich użytkowników końcowych.]* *Uwaga: Nieuzasadnione użycie oznaczeń może wydłużyć czas odpowiedniej reakcji.*	
Czy incydent miał wpływ na realizację zadań publicznych? Jeśli tak, na jakie?	