Załącznik do zarządzenia Nr 11/2021
Wójta Gminy Słupca
z dnia 22 lutego 2021 r.

System cyberbezpieczeństwa w systemach informacyjnych Gminy Słupca oraz podległych lub nadzorowanych jednostek

Art.1. System cyberbezpieczeństwa w systemach informacyjnych Gminy Słupca obowiązuje w następujących podległych lub nadzorowanych jednostkach: Urząd Gminy Słupca, Gminny Zakład Wodociągów i Kanalizacji, Gminny Ośrodek Pomocy Społecznej w Słupcy, Centrum Usług Wspólnych Gminy Słupca, Szkoła Podstawowa w Drążnej, Szkoła Podstawowa w Kowalewie Opactwie, Szkoła Podstawowa w Koszutach, Zespół Szkolno-Przedszkolny w Cieninie Kościelnym, Zespół Szkolno-Przedszkolny w Cieninie Zabornym, Zespół Szkolno-Przedszkolny w Kotuni, Zespół Szkolno-Przedszkolny w Młodojewie.

Art.2.

1. Słownik pojęć

1) CSIRT GOV - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;

2) CSIRT MON - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;

3) CSIRT NASK - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy;

4) cyberbezpieczeństwo - odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;

5) incydent - zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;

6) incydent krytyczny - incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;

7) incydent istotny - incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania

dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz.Urz. UE L 26 z 31.01.2018, str. 48);

8) incydent w podmiocie publicznym - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny;

9) obsługa incydentu - czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu;

10) podatność - właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa;

11) ryzyko - kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;

12) szacowanie ryzyka - całościowy proces identyfikacji, analizy i oceny ryzyka;

13) system informacyjny - system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2020 r. poz. 346, 568 i 695), wraz z przetwarzanymi w nim danymi w postaci elektronicznej;

14) usługa cyfrowa - usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344), wymienioną w załączniku nr 2 do ustawy;

15) zagrożenie cyberbezpieczeństwa - potencjalną przyczynę wystąpienia incydentu;

16) zarządzanie incydentem - obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;

17) zarządzanie ryzykiem - skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka;

18) Krajowy system cyberbezpieczeństwa - zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów;

19) punkt kontaktowy - wyznaczona przez Wójta Gminy Słupca osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;

20) podmiot publiczny - jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1-6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2019 r. poz. 869, z późn. zm.

2. Punkt kontaktowy

1) Wójt Gminy Słupca zarządzeniem nr 70/2019 z dnia 01.10.2019 r. wyznaczył osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa - zwaną dalej "punktem kontaktowym".

2) Punkt kontaktowy powołany został dla wszystkich podmiotów wymienionych w artykule 1.

3) punkt kontaktowy dostępny jest za pośrednictwem: poczty elektronicznej kontaktksc@gminaslupca.pl, telefonicznie 697-028-583 lub 63 274-36-76.

Art.3. Obowiązki podmiotów

1. Kierownicy jednostek wymienionych w artykule 1. zobowiązani są do zapewnienia:

1) zarządzania incydentem,

2) zgłaszania incydentów w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia,

3) obsługi incydentu w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe,

4) osobom, na rzecz których zadanie publiczne jest realizowane, dostępu 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. Obowiązki określone w ustępie 1. punkt 4. należy realizować na podstawie opracowań własnych lub we współpracy z punktem kontaktowym.

Art.4. Zgłoszenie incydentu w podmiocie publicznym

1. Zgłoszenie incydentu, o którym mowa w artykule 3 ustęp 1 punkt 2 przekazuje się w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej-przy użyciu innych dostępnych środków komunikacji.

2. Incydenty zgłasza się do punktu kontaktowego, który to przekazuje zgłoszenia do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

3. Zgłoszenie incydentu zawiera:

1) dane podmiotu zgłaszającego, w tym nazwę podmiotu, numer we właściwym rejestrze, siedzibę i adres;

2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby składającej zgłoszenie;

3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;

4) opis wpływu incydentu w podmiocie publicznym na realizowane zadanie publiczne, w tym:

a) wskazanie zadania publicznego, na które incydent miał wpływ,

b) liczbę osób, na które incydent miał wpływ,

c) moment wystąpienia i wykrycia incydentu oraz czas jego trwania,

d) zasięg geograficzny obszaru, którego dotyczy incydent,

e) przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego;

5) informacje o przyczynie i źródle incydentu;

6) informacje o podjętych działaniach zapobiegawczych;

7) informacje o podjętych działaniach naprawczych;

8) inne istotne informacje.

4. W zgłoszeniu incydentu przekazywane są informacje znane w chwili dokonywania zgłoszenia, które uzupełnia się w trakcie obsługi incydentu w podmiocie publicznym.

5. Punkt kontaktowy dokonuje zgłoszeń incydentów i przekazywania informacji do właściwego CSIRT w postaci elektronicznej albo przy użyciu innych środków komunikacji - w przypadku braku możliwości dokonania zgłoszenia albo przekazania ich w postaci elektronicznej.

6. Przekazywanie informacji i komunikacja z CSIRT MON, CSIRT NASK i CSIRT GOV, o których mowa w ustępie 5. odbywają się zgodnie z komunikatami publikowanymi w biuletynach informacji publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego.

7. Podmiot publiczny może przekazywać do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacje:

1) o innych incydentach;

2) o zagrożeniach cyberbezpieczeństwa;

3) dotyczące szacowania ryzyka;

4) o podatnościach;

5) o wykorzystywanych technologiach.

8. Informacje, o których mowa w ustępie 7 przekazywane są w postaci elektronicznej, a w przypadku braku możliwości przekazania ich w postaci elektronicznej - przy użyciu innych dostępnych środków komunikacji.

Art.5. Ochrona informacji i danych

1. W zgłoszeniu, o którym mowa w artykule 4. podmiot publiczny, przekazuje, w niezbędnym zakresie, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do realizacji zadań właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

2. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może zwrócić się do podmiotu publicznego, o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań.

3. W zgłoszeniu podmiot publiczny, oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

4. Do udostępniania informacji o podatnościach, incydentach i zagrożeniach cyberbezpieczeństwa oraz o ryzyku wystąpienia incydentów nie stosuje się ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2019 r. poz. 1429 oraz z 2020 r. poz. 695).

5. Nie udostępnia się informacji przetwarzanych na podstawie ustawy, jeżeli ich ujawnienie naruszyłoby ochronę interesu publicznego w odniesieniu do bezpieczeństwa lub porządku publicznego, a także negatywnie wpłynęłoby na prowadzenie postępowań przygotowawczych w sprawie przestępstw, ich wykrywania i ścigania.

WÓJT GMINY
Grażyna Kazuś