**Instrukcja zarządzania incydentami w zakresie systemu cyberbezpieczeństwa w *Szkole Podstawowej nr 2 im. Marii Konopnickiej w Czeladź,***

 ***41-250 Czeladź, ul. Szkolna 6***

W związku z realizacją wytycznych ustawy z dnia 5 lipca 2018 roku (Dz.U.2018.1560) o krajowym systemie cyberbezpieczeństwa w ***Szkole Podstawowej nr 2 im. Marii Konopnickiej w Czeladź, 41-250 Czeladź, ul. Szkolna 6***(dalej: **SP2** ) wprowadzona zostaje procedura mająca na celu prawidłowe wywiązanie się z nałożonych obowiązków w zakresie cyberbezpieczeństwa w **SP2** określająca zasady postępowania w chwili wystąpienia zagrożenia lub ataku, która przedstawia się następująco:

1. Do monitorowania przypadków mogących mieć negatywny wpływ na cyberbezpieczeństwo, wyznacza się Informatyka w SP2 w osobie: **Pana Pawła Jaskółkę**  przy czym każdy pracownik Jednostki, który zauważy wystąpienie zdarzeń (zachowań w obsługiwanych systemach) mogących wskazywać na ingerencję w system osób trzecich, zobowiązany jest zawiadomić Kierownika Jednostki.
2. Informatyk monitoruje w szczególności wystąpienie z poziomu Internetu i/lub domeny przypadków:
3. skanowania,
4. spamu przesyłanego za pośrednictwem polskich serwerów,
5. ataków typu DoS (Denial of Service) i DDoS (Distributed Denial of Service),
6. włamań i prób włamania.
7. Informatyk reaguje na każde zgłoszenie dokonane przez pracownika Jednostki dotyczące zdarzeń mogących wskazywać na cyberatak, lub inną formę ingerencji w systemy eksploatowane
w Jednostce, która wskazuje na niekontrolowane działanie osób trzecich oraz weryfikuje zgłoszenie
i podejmuje stosowne działania, o których mowa w pkt. 5.
8. Na podstawie opublikowanego corocznego raportu CERT Polska z 2018 roku (<https://www.cert.pl/news/single/zgloszenia-i-incydenty-w-2018-roku/>), wykaz incydentów, w tym incydentów występujących najczęściej ze szczegółowym podziałem na poszczególne kategorie według klasyfikacji eCSIRT.net[[1]](#footnote-2)przedstawia tabela 1.
9. Incydent w podmiocie publicznym **– SP2** ,który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego Informatyk zgłasza niezwłocznie:
10. Kierownikowi Jednostki, w celu umożliwienia realizacji obowiązku wynikającego z art. 22 ust. 1 pkt 2 Ustawy o krajowym systemie cyberbezpieczeństwa tj. zgłoszenia incydentu niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV zawierającego informacje, o których mowa w *załączniku nr 1* do niniejszej instrukcji.
11. Inspektorowi ochrony danych (IOD) w **SP2** na adres poczty elektronicznej: iodo@marwikpoland.pl poprzez przesłanie wypełnionego formularza stanowiącego *załącznik nr 1* do niniejszej instrukcji, oraz telefonicznie na numer kom: 694 167 023.

IOD dokonuje ustalenia czy zidentyfikowany incydent nie stanowi jednocześnie naruszenia ochrony danych osobowych, a w konsekwencji czy nie wymaga podjęcia stosownych działań w tym zakresie tj. oceny wagi ryzyka naruszenia praw i wolności osób fizycznych, oceny zasadności odnotowania incydentu w rejestrze incydentów
i naruszeń, zgłoszenia naruszenia do PUODO, i/lub zawiadomienia osób fizycznych których dane dotyczą.

*Tabela 1. Wykaz incydentów w podziale na kategorie wg klasyfikacji eCSIRT.net*

|  |  |
| --- | --- |
| **Obraźliwe i nielegalne treści**  | **Spam** |
|  | Dyskredytacja, obrażanie |
|  | Pornografia dziecięca, przemoc |
|  | Niesklasyfikowane |
| **Złośliwe oprogramowanie** | **Wirus** |
|  | **Robak sieciowy** |
|  | **Koń trojański** |
|  | **Oprogramowanie szpiegowskie** |
|  | **Dialer** |
|  | **Rootkit** |
|  | Niesklasyfikowane |
| **Gromadzenie informacji** | Skanowanie |
|  | Podsłuch |
|  | Inżynieria społeczna |
|  | Niesklasyfikowane |
| **Próby włamań**  | Wykorzystanie znanych luk systemowych |
|  | Próby nieuprawnionego logowania |
|  | Wykorzystanie nieznanych luk systemowych |
|  | Niesklasyfikowane |
| **Włamania** | Włamanie na konto uprzywilejowane |
|  | Włamanie na konto zwykłe |
|  | Włamanie do aplikacji |
|  | Bot |
|  | Niesklasyfikowane |
| **Dostępność zasobów**  | Atak blokujący serwis (DoS) |
|  | Rozproszony atak blokujący serwis (DDoS) |
|  | Sabotaż komputerowy |
|  | Przerwa w działaniu usług (niezłośliwe) |
|  | Niesklasyfikowane |
| **Atak na bezpieczeństwo informacji** | Nieuprawniony dostęp do informacji |
|  | Nieuprawniona zmiana informacji |
|  | Niesklasyfikowane |
| **Oszustwa komputerowe** | Nieuprawnione wykorzystanie zasobów |
|  | Naruszenie praw autorskich |
|  | Kradzież tożsamości, podszycie się |
|  | **Phishing** |
|  | Niesklasyfikowane |
| **Podatne usługi** | Otwarte serwisy podatne na nadużycia |
|  | Niesklasyfikowane |
| **inne** | **…**  |

##### **Załącznik 2**

##### **FORMULARZ ZGŁOSZENIA INCYDENTU**

##### **Dane osoby dokonującej zgłoszenia:**

|  |  |
| --- | --- |
| Imię i nazwisko  |  |
| Stanowisko służbowe |  |
| Kontakt (e-mail, nr tel.)  |  |

**Czy incydent miał/ma wpływ na realizację zadań publicznych? Jeśli tak, na jakie?**

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

**Dokładna lub przybliżona liczba osób, na które ma wpływ incydent?**

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

**Moment wystąpienia i wykrycia incydentu oraz przybliżony czas jego trwania**

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

**Zasięg geograficzny obszaru którego dotyczy incydent**

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

**Skutki oddziaływania incydentu na systemy informacyjne w Podmiocie**

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

**Informacje o przyczynie i źródle incydentu**

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

**Opis przebiegu incydentu**(najdokładniej jak to możliwe)

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

**Informacje o podjętych działaniach zapobiegawczych**

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

**Informacje o podjętych działaniach naprawczych**

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

**Inne istotne informacje**

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

**Wyciąg z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa**

**Rozdział 5**

Obowiązki podmiotów publicznych

**Art. 21**.

**1**. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu

informacyjnego jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów
z podmiotami krajowego systemu cyberbezpieczeństwa.

**2.** Organ administracji publicznej może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów
z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki jemu podległe lub przez niego nadzorowane.

**3.** Jednostka samorządu terytorialnego może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów

z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne.

**Art. 22.**

**1**. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemuinformacyjnego:

1) zapewnia zarządzanie incydentem w podmiocie publicznym;

2) zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, dowłaściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;

3) zapewnia obsługę incydentu w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRTMON, 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;

5) przekazuje do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV dane osoby, o której mowa w art. 21,obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

**2.** Zgłoszenie, o którym mowa w ust. 1 pkt 2, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

**Art. 23.**

**1.** Zgłoszenie, o którym mowa w art. 22 ust. 1 pkt 2, 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 systemyinformacyjne 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.

**2.** Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu w podmiocie publicznym.

1. Projekt współpracy zespołów CSIRT [↑](#footnote-ref-2)