MIEJSKI OŚRODEK POMOCY
SPOŁECZNEJ w DĘBICY
39-200 Dębica, ul. Akademicka 12
tel./fax (014) 670 50 06, 681 35 90, 681 35 91
MOPS.KP.021/36/2020

Zarządzenie Nr 36/2020
z dnia 18 maja 2020 roku
Dyrektora Miejskiego Ośrodka Pomocy Społecznej w Dębicy

w sprawie: wprowadzenia Procedur reagowania na incydenty cyberbezpieczeństwa w Miejskim Ośrodku Pomocy Społecznej w Dębicy.

Na podstawie art. 22 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560 ze zm.), zarządzam, co następuje:

§ 1

Wprowadzam Procedury reagowania na incydenty cyberbezpieczeństwa w Miejskim Ośrodku Pomocy Społecznej w Dębicy, będące załącznikiem do niniejszego Zarządzenia.

§ 2

Zobowiązuję Kierowników Działów do zapoznania wszystkich podległych pracowników z Procedurami, o których mowa w § 1.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Dębica, 18 maj 2020 r.

DYREKTOR
Miejskiego Ośrodka Pomocy Społecznej
w Dębicy
mgr Małgorzata Kędzior

Załącznik do Zarządzenia Nr 36/2020
z dnia 18 maja 2020 r.

PROCEDURY REAGOWANIA NA INCYDENTY CYBERBEZPIECZEŃSTWA W MIEJSKIM OŚRODKU POMOCY SPOŁECZNEJ W DĘBICY

§ 1

Podstawowe pojęcia:

1. **CSIRT NASK** - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy.
2. **Cyberbezpieczeństwo** - odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
3. **Dyrektor** – Dyrektor Miejskiego Ośrodka Pomocy Społecznej w Dębicy.
4. **Incydent** - zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
5. **Incydent w podmiocie publicznym** - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.
6. **MOPS** – Miejski Ośrodek Pomocy Społecznej w Dębicy.
7. **Obsługa incydentu** - czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydent.

§ 2

1. W przypadku ujawnienia incydentu każda osoba zatrudniona w MOPS zobowiązana jest niezwłocznie powiadomić o tym fakcie Dyrektora.
2. Osoba zatrudniona w MOPS, jeżeli otrzymała na służbową skrzynkę e-mail podejrzaną wiadomość, w której została poproszona np. o podanie swoich danych logowania, bądź ściągnięcie dziwnie wyglądającego załącznika i inne, należy zgłosić niezwłocznie, jak w ust. 1.
3. Dzięki zgłoszeniom, o którym mowa w ust. 1 i 2 Dyrektor może lepiej szacować ryzyko i reagować na zagrożenie.

4. Osoba wyznaczona do kontaktów z CSIRT NASC, zgłasza do CSIRT NASC incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego wykonywanego w MOPS niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia.
5. Zgłoszenie następuje poprzez dedykowany formularz, dostępny na stronie internetowej https://incydent.cert.pl/, a w przypadku braku możliwości przekazania go w postaci elektronicznej - przy użyciu innych dostępnych środków komunikacji.

§ 3

1. Zgłoszenie, o którym mowa w § 2 ust. 4, zawiera w szczególności:

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) o przyczynie i źródle incydentu;
6) informacje o podjętych działaniach zapobiegawczych;
7) informacje o podjętych działaniach naprawczych;
8) inne istotne informacje.

2. Osoba wyznaczona do kontaktów z CSIRT NASC jest osobą obsługującą incydent, przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu w podmiocie publicznym, nie czeka na zebranie wszystkich informacji.

3. Osoba wyznaczona do kontaktów z CSIRT NASC, w zgłoszeniu przekazuje w niezbędnym zakresie, informacje stanowiące tajemnice prawnie chronione, gdy jest to konieczne do realizacji zadań CSIRT NASK.
4. Osoba wyznaczona do kontaktów z CSIRT NASC może uzupełnić zgłoszenie o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, jeżeli zwróci się do MOPS - CSIRT NASC.
5. W zgłoszeniu osoba wyznaczona do kontaktów z CSIRT NASC, oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.
6. W przypadku braku wszystkich powyższych informacji osoba wyznaczona do kontaktów z CSIRT NASC, jest zobowiązana przekazać informacje znane jej w chwili dokonywania zgłoszenia, które następnie uzupełnia w trakcie obsługi incydentu.
7. Informacje przekazywane w późniejszym terminie powinny być przekazywane niezwłocznie zaraz po ich ustaleniu. Nie należy czekać aż do momentu ustalenia wszystkich informacji, po każdym ustaleniu cząstkowych informacji należy je przesłać do właściwego CSIRT NASC.

§ 4

1. W przypadku podejrzanej wiadomości e-mail (podejrzane załączniki, phishing, szantaż) - należy zapisać podejrzaną wiadomość do pliku .EML. Nie otwierać załącznika.
2. W przypadku próby oszustwa, próby podszywania się – należy zebrać informacje na ten temat, m.in. skąd posiadasz taką informację, korespondencję - jeżeli była, zgłoszenie na Policję - jeżeli było, nr konta - jeżeli dokonano oszustowi płatności i in.
3. W przypadku złośliwego oprogramowania, wirusów, plików zaszyfrowanych ransomware – należy spakować podejrzany plik do archiwum formacie .rar, .zip, .7z. Należy zabezpieczyć archiwum hasłem infected.
4. W przypadku błędów w oprogramowaniach lub aplikacjach internetowych, tzw. podatnościach, należy przygotować techniczne wyjaśnienie charakteru takiej podatności.
5. W przypadku nielegalnych treści w Internecie, mających wpływ na realizację zadania publicznego MOPS – należy zebrać informacje i link/linki gdzie te treści znajdują się.

6. W przypadku innych incydentów, które nie pasują do przykładów ust. 1-5, a którymi mogą być np. (skanowanie, atak DDoS, nieuprawnione próby logowania), należy zabezpieczyć logi z tych zdarzeń.
7. W czynnościach, o których mowa w ust. 1-6 pomocy udziela osoba wyznaczona do kontaktów z CSIRT NASC.

§ 5

1. Każda osoba zatrudniona w MOPS zobowiązana jest do współpracy z osobą obsługującą incydent i udzielania wyczerpujących informacji.
2. Osoba obsługująca incydent zobowiązana jest do stałego raportowania Dyrektorowi przebiegu obsługi zgłoszonego incydentu.

DYREKTOR
Miejskiego Ośrodka Pomocy Społecznej
w Dobrej
mgr Małgorzata Kędzior