ZARZĄDZENIE NR 16/2023
BURMISTRZA MIASTA I GMINY FROMBORK
z dnia 08 lutego 2023 r.

w sprawie wprowadzenia w Urzędzie Miasta i Gminy we Fromborku procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem

Na podstawie art. 22 ust. 1 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2022 r. poz. 1863 z późn. zm.) Burmistrz Miasta i Gminy Frombork zarządza, co następuje:

§ 1.

Wprowadza się w Urzędzie Miasta i Gminy Frombork procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem, stanowiące załącznik do zarządzenia.

§ 2.

1. Zobowiązuje się wszystkich pracowników Urzędu Miasta i Gminy Frombork do zapoznania się z procedurami, o których mowa w § 1.
2. Pisemne oświadczenie o zapoznaniu się i przestrzeganiu procedur należy złożyć w Referacie Organizacyjnym Urzędu Miasta i Gminy we Fromborku.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta i Gminy we Fromborku

/-/ Zbigniew Pietkiewicz

Załącznik Nr 1 do zarządzenia Nr 16/2023
Burmistrza Miasta i Gminy Frombork
z dnia 8 lutego 2023 r.

PROCEDURA ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI I CYBERBEZPIECZEŃSTWEM

Rozdział 1
Postanowienia ogólne

§ 1. Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływów przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność Urzędu Miasta i Gminy Frombork.

§ 2. Podstawą prawną do opracowania i wdrożenia procedury jest:
1) art. 22 ust. 1 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
2) § 20 ust. 2 pkt. 13 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247).

§ 3. Definicje użyte w niniejszej procedurze oznaczają:
1) Inspektor Ochrony Danych - osoba wyznaczona przez Administratora Danych Osobowych zwana dalej "IOD";
2) Administrator Systemów Informatycznych - osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych zwana dalej "ASI";
3) Administrator Danych Osobowych "ADO" - Gmina Frombork reprezentowana przez Burmistrza Miasta i Gminy Frombork.

Rozdział 2
Kategorie incydentów

§ 4. Incydent bezpieczeństwa informacji oraz cyberbezpieczeństwa to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych oraz który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny. Jego przyczyną mogą być:
1) zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp), którego wystąpienie może spowodować zniszczenie lub uszkodzenie

infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenie ciągłości pracy systemów nie powodując naruszenia poufności danych;

2) zdarzenie losowe wewnętrzne (np. błędy w oprogramowaniu, awarie sprzętu itp.), które mogą powodować zakłócenia ciągłości pracy systemów, a także prowadzić do zniszczenia lub utraty danych;
3) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.

§ 5. Incydentami bezpieczeństwa informacji w szczególności są:
1) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
2) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
3) naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.

§ 6. Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą dotyczyć:
1) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwego postępowania z dokumentacją papierową;
2) działania szkodliwego oprogramowania;
3) próby omijania systemów zabezpieczeń;
4) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
5) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
6) zniszczenia lub kradzieży nośników danych;
7) prób wyłudzeń informacji;
8) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
9) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
10) naruszenia zasad obowiązujących w Urzędzie Miasta i Gminy Frombork dotyczących bezpieczeństwa informacji, w tym danych osobowych.

Rozdział 3
Zakres obowiązywania procedury zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem

§ 7. Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem obowiązuje w Urzędzie Miasta i Gminy Frombork.

Rozdział 4
Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem

§ 8. 1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie Administratora Danych Osobowych i Administratora Systemów Informatycznych oraz Inspektora Ochrony Danych (jeżeli incydent może dotyczyć danych osobowych).

2. Zgłoszenia dokonuje się telefonicznie lub osobiście. Zgłoszenie należy potwierdzić szczegółową notatką służbową, którą przekazuje się do ASI.

3. Notatka musi zawierać następujące informacje:
1) imię i nazwisko zgłaszającego;
2) stanowisko oraz komórkę organizacyjną;
3) dokładne miejsce oraz datę wystąpienia incydentu;
4) opis incydentów w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego.

§ 9. Brak umiejętności poprawnego rozpoznania incydentu przez osobą zgłaszającą nie może być przyczyną zaniechania zgłoszenia.

§ 10. W przypadku nieobecności ASI incydent należy zgłosić do ADO lub osoby wskazanej przez ADO.

Rozdział 5.

Podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem

§ 11. 1. Zgłoszenie incydentu rejestrowane jest przez ASI i przechowywane w teczce.
2. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.).
3. Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia.
4. W przypadku kiedy zgłoszenie zakwalifikowane zostało jako incydent bezpieczeństwa informacji lub cyberbezpieczeństwa, ASI dokonuje jego oceny istotności.
5. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
1) powstałe szkody będące wynikiem incydentu;
2) wpływ incydentu na działanie systemów;
3) wpływ incydentu na ciągłość działania Urzędu Miasta i Gminy Frombork;
4) koszty usunięcia skutków incydentu;
5) szacowany czas naprawy skutków wywołanych incydentem;
6) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
6. Zakwalifikowanie zgłoszenia jako „fałszywy alarm” kończy postępowanie, o czym ASI informuje zgłaszającego.

7. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, ASI podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
8. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego, ASI lub ADO (w porozumieniu z IOD), nie później niż w ciągu 24 godzin od momentu wykrycia, zgłasza incydent do właściwego CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy ul. Kolska 12, 01-045 Warszawa).
9. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. W przypadku braku możliwości przekazania zgłoszenia w sposób elektroniczny należy dokonać go przy użyciu innych dostępnych środków komunikacji tj. telefon, fax.
10. W zgłoszeniu przekazuje się informacje zgodne z formularzem oraz zgodnie z wymogami art. 23 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
11. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa informacji oraz cyberbezpieczeństwa, ADO podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie w zależności od wagi incydentu może powiadomić organy ścigania.

Rozdział 6.
Reagowanie na awarię

§ 12. Jeśli awaria dotyczy systemu krytycznego i może mieć wpływ na wydajność systemów teleinformatycznych, ASI informuje ADO.

§ 13. 1. W przypadku gdy awarię można usunąć samodzielnie, ASI dokonuje naprawy. Do podstawowych działań w takim wypadku zaliczyć można:
1) wymianę stacji roboczej;
2) wymianę podzespołów w stacji roboczej;
3) wymianę urządzenia sieciowego;
4) odtworzenie danych z kopii zapasowej.

§ 14. 1. W przypadku gdy ASI uzna, iż nie jest w stanie samodzielnie usunąć awarii, informację dotyczącą awarii przekazuje do producenta sprzętu lub oprogramowania.
2. Jeżeli konieczność naprawy dotyczy sprzętu wówczas naprawa dokonywana jest przez producenta w obecności ASI.
3. Jeżeli konieczność naprawy dotyczy oprogramowania, wgrywana poprawka powinna zostać pozytywnie zweryfikowana w środowisku testowym.

Rozdział 7.
Reagowanie na błędy w oprogramowaniu

§ 15. Po otrzymaniu zgłoszenia dotyczącego wystąpienia błędu systemowego lub aplikacyjnego w oprogramowaniu ASI diagnozuje przyczyny błędu oraz podejmuje działania zmierzające do rozwiązania

problemu. Do podstawowych działań w takim wypadku zaliczyć można:
1) wykorzystanie bazy wiedzy o błędach w oprogramowaniu;
2) zmianę konfiguracji oprogramowania;
3) ponowną instalację oprogramowania;
4) instalację nowej wersji oprogramowania.

§ 16. W przypadku gdy ASI, nie jest w stanie samodzielnie naprawić błędu w oprogramowaniu, przekazuje tę informację do producenta oprogramowania (pracownik powinien w tym przypadku postępować zgodnie z umowami serwisowymi lub licencjami).

§ 17. W przypadku gdy zaistnieje powód wskazujący na to, że przyczyną błędu w oprogramowaniu było naruszenie bezpieczeństwa, ASI informuje o tym fakcie ADO.

Rozdział 8.
Reagowanie na wykrycie złośliwego kodu mobilnego

§ 18. Po otrzymaniu zgłoszenia dotyczącego pojawienia się złośliwego kodu mobilnego na stacji roboczej, serwerze lub samodzielnemu wejściu w posiadanie wiedzy o takim zdarzeniu, ASI w pierwszej kolejności powinien:
1) odłączyć komputer od sieci komputerowej;
2) sprawdzić aktualność baz danych wirusów (jeżeli są nieaktualne należy dokonać ich aktualizacji);
3) sprawdzić poprawność działania oprogramowania antywirusowego (jeżeli oprogramowanie nie działa poprawnie należy je odinstalować i zainstalować ponownie);
4) uruchomić pełne skanowanie komputera i nośników informacji, z którymi mógł mieć styczność.

§ 19. Jeżeli atak złośliwego kodu mobilnego nie został zneutralizowany przez oprogramowanie antywirusowe, ASI nakazuje użytkownikowi przerwanie pracy. Następnie dokonuje ponownej instalacji systemy operacyjnego i oprogramowania oraz odzyskania danych z kopii zapasowych. Kopie zapasowe przed wgraniem do komputera należy sprawdzić programem antywirusowym.

§ 20. W przypadku gdy zaistnieje powód wskazujący na to, że przyczyną ataku złośliwego kodu mobilnego było naruszenie bezpieczeństwa, ASI informuje o tym fakcie ADO