ZARZĄDZENIE NR 3/2022
WÓJTA GMINY TUROŚL

z dnia 17 stycznia 2022 r.

w sprawie wprowadzenia w Urzędzie Gminy Turośl procedury zarządzania incydentami cyberbezpieczeństwa

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2022 r. poz. 559) i art. 22 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369 z późn. zm.), zarządzam co następuje:

§ 1. Wprowadzam Procedurę zarządzania incydentami z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Gminy Turośl stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierzam Administratorowi Systemów Informatycznych, Inspektorowi Ochrony Danych, kierownikom komórek organizacyjnych oraz pracownikom zajmującym samodzielne stanowiska pracy.

§ 3. Nadzór nad wykonaniem zarządzenia powierzam Administratorowi Systemów Informatycznych.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.

Wójt Gminy

Piotr Niedbała

Załącznik do zarządzenia Nr 3/2022

Wójta Gminy Turośl

z dnia 17 stycznia 2022 r.

PROCEDURA ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI I CYBERBEZPIECZEŃSTWEM

Rozdział 1.
Postanowienia ogólne

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

§ 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;

§ 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 Turośl reprezentowana przez Wójta Gminy Turośl;
4) Incydent - zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
5) 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;

Rozdział 2.
Kategorie incydentów

§ 4. Incydent 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. Przyczyny incydentów mogą dotyczyć:

1) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie 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 Gminy w Turośli dotyczących bezpieczeństwa informacji.

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

§ 6. Procedura zarządzania incydentami obowiązuje w Urzędzie Gminy w Turośli.

Rozdział 4.
Zapobieganie incydentom

§ 7. Utrzymywanie liczby incydentów na odpowiednio niskim poziomie jest bardzo ważne dla ochrony procesów w urzędzie. Jeśli środki bezpieczeństwa są niewystarczające, może dojść do większej liczby incydentów, przytłaczających zespół reagowania na incydenty. Może to prowadzić do powolnych i niepełnych odpowiedzi, co przekłada się na większy negatywny wpływ na działalność Urzędu (np. większe szkody, dłuższe okresy niedostępność usług i danych).

W celu zapobiegania występowaniu incydentom ASI podejmuje wszelkie niezbędne działania, w szczególności:

1) **Szacowanie ryzyka.** Okresowe oceny ryzyka systemów i aplikacji powinny określać, jakie ryzyka stwarzają kombinacje zagrożeń i podatności. Powinno obejmować to zrozumienie odpowiednich zagrożeń, w tym zagrożeń specyficznych dla organizacji. Każdemu ryzyku należy nadać priorytet, a ryzyko można ograniczać, przenosić lub akceptować do czasu osiągnięcia akceptowalnego ogólnego poziomu ryzyka

2) **Bezpieczeństwo hosta.** Wszystkie hosty powinny być odpowiednio zabezpieczone przy użyciu standardowych konfiguracji. Oprócz utrzymywania każdego hosta odpowiednio zaktualizowanego za pomocą poprawek, hosty powinny być skonfigurowane zgodnie z zasadą najniższych uprawnień - przyznając użytkownikom tylko te uprawnienia, które są niezbędne do wykonywania ich autoryzowanych zadań. Hosty powinny mieć włączone przeprowadzanie audytu i powinny rejestrować istotne zdarzenia związane z bezpieczeństwem. Bezpieczeństwo hostów i ich konfiguracji powinno być stale monitorowane.

3) **Bezpieczeństwo sieci.** Sieć powinna być skonfigurowana tak, aby odmawiała wszelkiej aktywności, która nie jest wyraźnie dozwolona. Obejmuje to zabezpieczenie wszystkich punktów połączeń, takich jak wirtualne sieci prywatne (VPN) i dedykowane połączenia z innymi organizacjami.

4) **Zapobieganie złośliwemu oprogramowaniu.** Oprogramowanie do wykrywania i powstrzymywania złośliwego oprogramowania powinno być wdrażane w całej organizacji. Ochrona przed złośliwym oprogramowaniem powinna być wdrażana na poziomie hosta (np. systemów operacyjnych serwerów i stacji roboczych), na poziomie serwera aplikacji (np. serwera poczty elektronicznej, serwerów proxy) i na poziomie klienta aplikacji (np. klientów poczty e-mail, komunikatorów internetowych).

5) **Świadomość i szkolenie użytkowników.** Użytkownicy powinni być świadomi zasad i procedur dotyczących właściwego korzystania z sieci, systemów i aplikacji. Zatwierdzone wnioski z poprzednich incydentów należy również udostępnić użytkownikom, aby mogli zobaczyć, jak ich działania mogą wpłynąć na organizację. Poprawa świadomości użytkowników w zakresie incydentów powinna zmniejszyć częstotliwość incydentów.

Rozdział 5.
Zgłaszanie incydentów

§ 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 do ASI.

3. Notatka musi zawierać następujące informacje:

1) imię i nazwisko zgłaszającego,

2) stanowisko oraz komórka organizacyjna,

3) dokładne miejsce oraz datę wystąpienia incydentu,

4) opis incydentów 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 6.
Podejmowanie działań w związku ze zgłaszanymi incydentami

§ 11. 1. Zgłoszenie incydentu rejestrowane jest przez ASI.

2. ASI prowadzi dokumentację związaną z incydentem lub incydentem krytycznym, w szczególności:

1) Informacje identyfikacyjne (np. lokalizacja, numer seryjny, numer modelu, nazwa hosta, adresy sprzętowe MAC i adresy IP komputera).

2) Nazwisko, stanowisko i numer kontaktowy każdej osoby, która zebrała lub zajmowała się materiałami dowodowymi podczas prowadzonego dochodzenia.

3) Godzina i data (w tym strefa czasowa) każdego przypadku postępowania dowodowego.

4) Lokalizacje, w których przechowywano dowody.

3. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora).

4. Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia.

5. W przypadki kiedy zgłoszenie zakwalifikowane zostało jako incydent, ASI dokonuje jego oceny istotności.

6. 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 w Turośli;

4) koszty usunięcia skutków incydentu;

5) szacowany czas naprawy skutków wywołanych incydentem;

6) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.

7. Zakwalifikowanie zgłoszenia jako „fałszywy alarm” kończy postępowanie, o czym ASI informuje zgłaszającego.

8. W przypadku zakwalifikowania zdarzenia jako incydentu, ASI podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.

9. 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).

10. 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.

11. 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.

12. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu, ADO podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie w zależności od wagi incydentu może powiadomić organy ścigania.

Rozdział 7.
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 lub serwis w obecności ASI.

3. Jeżeli konieczność naprawy dotyczy oprogramowania, wgrywana poprawka powinna zostać pozytywnie zweryfikowana w środowisku testowym.

Rozdział 8.
Reagowanie na błędy w oprogramowaniu

§ 15. 1. 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.

2. W przypadku gdy ASI, iż 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).

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

Rozdział 9.
Reagowanie na wykrycie złośliwego kodu mobilnego

§ 16. 1. 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.

2. 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.

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

Rozdział 10.
Działania podejmowane po wystąpieniu incydentu

§ 17. 1. ASI dokonuje analizy incydentu pod kątem przyczyn wystąpienia i skutków.

2. ASI podejmuje czynności zmierzające do wdrożenia działań naprawczych i następczych, mających na celu minimalizację prawdopodobieństwa wystąpienia identycznych lub podobnych incydentów.

3. ASI jest odpowiedzialny za opracowanie raportu z incydentu oraz podjętych w jego wyniku działań następczych.

4. Wystąpienie incydentów i incydentów krytycznych oraz ich następstwa należy uwzględnić w procesie szacowania ryzyka.