ZARZĄDZENIE NR 10/2023
STAROSTY RYPIŃSKIEGO
z dnia 10 marca 2023 r.

w wprowadzenia procedury reagowania na incydenty bezpieczeństwa komputerowego w Starostwie Powiatowym w Rypinie

Na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz.1863, poz. 2666), w związku z uchwałą Nr 447/2021 Zarządu Powiatu w Rypinie z dnia 8 września 2021 w sprawie wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz uchwałą Nr 690/2023 Zarządu Powiatu w Rypinie z dnia 4 stycznia 2023 r. w sprawie zmiany Uchwały Nr 447/2021 Zarzadu Powiatu w Rypinie z dnia 8 wrzesnia 2021 r. w sprawie wyznaczenia osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa **zarządzam, co następuje:**

§ 1.

1. Wprowadza się procedury reagowania na incydenty bezpieczeństwa informatycznego w Starostwie Powiatowym w Rypinie w brzmieniu stanowiącym załącznik Nr 1 do niniejszego zarządzenia.
2. Zobowiązuje się pracowników Starostwa Powiatowego w Rypinie do zapoznania i stosowania w/w procedur.

§ 2.

Wykonanie zarządzenia powierza się Sekretarzowi Powiatu Rypińskiego

§ 3.

Zarządzanie wchodzi w życie z dniem podjęcia.

Załącznik Nr 1
do Zarządzenia Nr10/2023
Starosty Rypińskiego
z dnia 10 marca 2023 r.

Procedura reagowania na incydenty bezpieczeństwa informatycznego w Starostwie Powiatowym w Rypinie

I. Postanowienia ogólne, definicje

1. Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność Starostwa Powiatowego w Rypinie.
2. Podstawą prawną do opracowania i wdrożenia dokumentu jest:
   a) art. 22 ust.1 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
   b) § 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.
3. **Administrator Danych Osobowych** – Starostwo Powiatowe w Rypinie w imieniu którego działa **Starosta Rypiński.**
4. **Administrator Systemów Informatycznych (ASI)** – jest jednocześnie **Z-cą osoby wyznaczonej do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa** - zwany **w treści Z-ca Osoby wyznaczonej**. Dane kontaktowe: informatyk@powiatrypinski.pl.
5. **Incydent w podmiocie publicznym** - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.
6. **Incydent krytyczny** – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku prawnego, interesów międzynarodowych , interesów gospodarczych, działania instytucji publicznych, praw lub wolności obywatelskich lub życia i zdrowia ludzi,

klasyfikowany przez właściwy CSIRT NASK.

7. **Inspektor Ochrony Danych** (IOD) - / osobą wyznaczoną do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Dane kontaktowe: ido@powiatrypinski.pl

II. Kategorie incydentów

1. Incydent 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.
2. Incydentami bezpieczeństwa informacji w szczególności są:
   a) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
   b) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
   c) naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.
3. Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą dotyczyć:
   a) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową;
   b) działania szkodliwego oprogramowania;
   c) próby omijania systemów zabezpieczeń;
   d) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
   e) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
   f) zniszczenia lub kradzieży nośników danych;
   g) próby wyłudzeń informacji;
   h) ataków socjotechnicznych , ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
   i) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
   j) naruszenia zasad obowiązujących w Urzędzie dotyczących bezpieczeństwa informacji, w tym danych osobowych.
4. Przykłady incydentów cyberbezpieczeństwa:
   a) podejrzana wiadomość e-mail: podejrzane załączniki: np. ,,PILNA FAKTURA", ,,OPLAC ZAMOWIENIE", phishing, szantaż,

b) próba oszustwa - próba podszywania się np. pod administratora w celu wyłudzenia haseł dostępu do sieci,
c) złośliwe oprogramowanie próbki wirusów lub pliki zaszyfrowane ransomware,
d) błędy w oprogramowaniu lub aplikacjach internetowych,
e) nielegalne treści: związane z rasizmem, ksenofobią, pornografią,
f) inne wzbudzające podejrzenia użytkownika sieci komputerowej.

III. Reagowanie na incydenty związanych z cyberbezpieczeństwem

1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie Inspektora Ochrony Danych/ Osobę wyznaczoną oraz Administratora Systemów Informatycznych.
2. IOD sporządza notatkę z zgłoszenia zawierającą następujące informacje:
   a) imię i nazwisko osoby zgłaszającej;
   b) stanowisko oraz komórka organizacyjna Starostwa Powiatowego w Rypinie;
   c) dokładne miejsce oraz datę wystąpienia incydentu;
   d) opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego.
3. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.
4. W przypadku dłuższej nieobecności IOD incydent należy zgłosić do Z-cy Osoby Wyznaczonej - ASI.
5. Administrator Systemu podejmuje natychmiastowe działania w celu zminimalizowania skutków nieuprawnionego dostępu do sieci komputerowej oraz współdział z Osobą wyznaczoną do kontaktu.

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

1. Zgłoszenie incydentu rejestrowane jest przez IOD i przechowywane w dokumentacji zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.). Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy

zgłoszenie zakwalifikowane zostało jako incydent cyberbezpieczeństwa, dokonywana jest jego ocena istotności.

2. Powyższe działania wykonuje IOD w porozumieniu z ASI.
3. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
   a) powstałe szkody będące wynikiem incydentu;
   b) wpływ incydentu na działanie systemów;
   c) wpływ incydentu na ciągłość działania Urzędu;
   d) koszty usunięcia skutków incydentu;
   e) szacowany czas naprawy skutków wywołanych incydentem;
   f) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
4. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm" kończy postępowanie, o czym IOD informuje zgłaszającego.
5. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z cyberbezpieczeństwem, IOD wspólnie z ASI podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
6. W przypadku stwierdzenia incydentu lub incydentu krytycznego IOD/Osoba wyznaczona lub osoba wyznaczona w zastępstwie (w przypadku nieobecności) nie później niż w ciągu **24 godzin** od momentu wykrycia zgłasza incydent do właściwego CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowego Instytutu Badawczego ul. Kolska 12, 01-045 Warszawa).
7. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym https://incydent.cert.pl . W przypadku braku możliwości przekazania go w sposób elektroniczny można zgłaszać przy użyciu innych dostępnych środków komunikacji (np. na numer telefonu +48223808274).
8. W zgłoszeniu przekazuje się informacje zgodnie z formularzem oraz zgodnie z treścią art. 23 ust. 1 ustawy z dnia 05 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
9. 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 mogą być powiadomione organy ścigania.