ZARZĄDZENIE Nr 402/2023

Burmistrza Sokółki

z dnia 10 lutego 2023 r.

w sprawie wprowadzenia Planu zarządzania incydentami w zakresie cyberbezpieczeństwa w Urzędzie Miejskim w Sokółce

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. z 2023.40 tj. z dnia 2023.01.05) i ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2022 poz. 1863 tj. 2022.09.05) zarządza, co następuje:

§ 1

W Urzędzie Miejskim w Sokółce wprowadza się Plan zarządzania incydentami w zakresie cyberbezpieczeństwa, stanowiący załącznik Nr 1 do niniejszego zarządzenia.

§ 2

Zobowiązuje się wszystkich pracowników Urzędu Miejskiego w Sokółce do stosowania i przestrzegania Planu zarządzania incydentami w zakresie cyberbezpieczeństwa.

§3

Wyznacza się ASI w Urzędzie Miejskim w Sokółce do monitorowania przypadków mogących mieć negatywny wpływ na cyberbezpieczeństwo.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

Ewa Kalikowska

10.02.2023

Marcin Puszko

Starszy informatyk

Piotr Romanowicz

Sekretarz

10.02.2023

POD WZGLĘDEM FORMALNO-PRAWNYM ZASTRZEŻEŃ NIE WNOSZĘ

RADCA PRAWNY

mgr Danuta Kowalczyk

10.02.2023 r.

Załącznik Nr 1 do
Zarządzenia Nr 402/2023 Burmistrza Sokółki
z dnia 10.02.2023r.
sprawie wprowadzenia
Planu zarządzania incydentami w zakresie cyberbezpieczeństwa
w Urzędzie Miejskim w Sokółce

1. Cel procedury.

Celem procedury Planu zarządzania incydentami w zakresie cyberbezpieczeństwa w Urzędzie Miejskim w Sokółce jest zapewnienie, że zdarzenia związane z bezpieczeństwem informacji oraz słabości systemów informacyjnych, są zgłaszane w sposób umożliwiający szybkie podjęcie działań korygujących.

2. Zakres stosowania.

Działania opisane w niniejszej procedurze obowiązują, we wszystkich wydziałach, referatach i pozostałych komórkach organizacyjnych urzędu. Niniejsza procedura jest elementem Polityki Bezpieczeństwa Informacji ustanowionej w Urzędzie.

3. Odpowiedzialność.

Odpowiedzialność za prawidłowe zgłoszenie incydentów dotyczących bezpieczeństwa infrastruktury informatycznej spoczywa na pracownikach Urzędu dokonujących zgłoszeń. ASI odpowiedzialny jest za rozwiązanie problemu lub zapobieżenie incydentowi działa zgodnie z niniejszą procedurą.
ASI jest odpowiedzialny za:
1) Niezwłoczne reagowanie na incydenty bezpieczeństwa informacji w określony i z góry ustalony sposób;
2) Ocenę istniejących i potencjalnych zagrożeń w zakresie bezpieczeństwa informacji;
3) Ocenę przyczyn i skutków incydentów naruszenia bezpieczeństwa informacji w tym gromadzenie materiału dowodowego;
4) Przygotowywanie propozycji działań korygujących i naprawczych oraz nadzór nad ich wprowadzaniem;
5) Dokonywanie okresowego przeglądu i aktualizacji Polityki Bezpieczeństwa Informacji;
6) Prowadzenie działań zmierzających do wzrostu świadomości w zakresie zapewnienia bezpieczeństwa informacji w Urzędzie;
7) Współpracę z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.

4. Klasyfikacja incydentów.

Podział zdarzeń

I) Zdarzenia losowe zewnętrzne (np.: klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, ciągłość pracy systemów zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2) Zdarzenia losowe wewnętrzne (np.: pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3) Zdarzenia zamierzone, świadome i celowe - stanowią najpoważniejsze zagrożenie naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zdarzenia te możemy podzielić na:
- nieuprawniony dostęp do danych z zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do danych z sieci wewnętrznej,
- nieuprawniony transfer danych,
- pogorszenie funkcjonowania sprzętu i oprogramowania (np.: działanie wirusów),
- bezpośrednie zagrożenie materialnych składników systemu (np.: kradzież sprzętu).

Przykłady zdarzeń które mogą być zakwalifikowane jako uzasadnione podejrzenie naruszenia bezpieczeństwa informacji:

I) Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.

2) Niewłaściwe parametry środowiska jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni).

3) Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.

4) Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.

5) Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikacje w systemie.

6) Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.

7) Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).

8) Nastąpiła niedopuszczalna manipulacja danymi w systemie.

9) Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą elementy systemu zabezpieczeń.

10) Praca w systemie lub w sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np.: praca w systemie lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.

11) Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.

12) Podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w niedozwolony sposób skasowano lub kopiowano dane osobowe.

13) Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania PBI (nie wylogowanie się, pozostawienie włączonego komputera po zakończeniu pracy, nie zamknięcie pokoju z komputerem, nie wykonywanie w ustalonych terminach kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)

14) Stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka)

5. Zgłaszanie incydentów

Pracownicy Urzędu mają obowiązek zgłaszać zauważone przez siebie incydenty oraz notować wszystkie szczegóły związane z incydentem.

Punktem kontaktowym jest Referat Organizacji Urzędu Miejskiego. Incydenty należy zgłaszać do ASI, przy czym każdy pracownik urzędu, który zauważy wystąpienie zadań mogących wskazywać na ingerencję w systemie osób trzecich, zobowiązany jest powiadomić Burmistrza Sokółki.

Zgłoszenie musi zawierać elementy wskazane w art. 23 ustawy o krajowym systemie cyberbezpieczeństwa, formularz zgłoszeniowy do wykorzystania znajduje się w pkt. 9 niniejszego planu.

6. Gromadzenie materiału dowodowego:

1) dla dokumentów papierowych: oryginał jest bezpiecznie przechowywany wraz z informacją, kto znalazł dokument, gdzie, kiedy i kto by był świadkiem tego zdarzenia; każde śledztwo może wykazać, że oryginał nie został naruszony

2) dla dokumentów na nośnikach komputerowych zaleca się: utworzenie obrazu lub kopii (zależnie od stosownych wymagań) wszelkich nośników wymiennych; zaleca się zapisanie informacji znajdujących się na dyskach twardych lub w pamięci komputera, aby zapewnić ich dostępność, zaleca się zachowanie zapisów wszelkich działań podczas procesu kopiowania oraz aby proces ten odbywał się w obecności

świadków; zaleca się przechowywanie oryginalnego nośnika i dziennika zdarzeń w sposób bezpieczny i nienaruszony (jeśli to niemożliwe, to co najmniej jeden obraz lustrzany lub kopię).
3) W przypadku, gdy zgłoszone zdarzenie nie zostało zaklasyfikowane jako incydent bezpieczeństwa informacji, ma charakter fałszywego alarmu Informatyk powiadamia zgłaszającego o zdarzeniu, że zdarzenie nie stanowi incydent bezpieczeństwa.
4) W przypadku stwierdzenia działań umyślnych i ustaleniu sprawcy incydentu przekazuje się wyniki analizy wraz z zabezpieczonym materiałem dowodowym Sekretarzowi Urzędu w celu wyciągnięcia konsekwencji dyscyplinarnych wobec sprawcy, ewentualnego zawiadomienia organów ścigania lub podjęcia kroków prawnych wobec osób trzecich.
5) Inicjuje się działania naprawcze zmierzające do zniwelowania szkód wyrządzonych przez incydent, wyciąga wnioski z każdego incydentu i określa jeśli to możliwe działania korygujące i zapobiegawcze w celu uniknięcia ponownego wystąpienia incydentu.
6) Na bieżąco dokumentuje się swoje działania na każdym z etapów procesu zarządzania incydentem w formie notatki. Obsługa incydentu kończy się raportem zatwierdzonym przez Sekretarza Urzędu zawierającym opis incydentu oraz wnioski co do działań na przyszłość.

7. Postępowanie z incydentami

Obsługa incydentu rozpoczyna się od jego dokładnego rozpoznania - ustalenia oznak naruszenia bezpieczeństwa, identyfikacji rodzaju incydentu, identyfikacji i zabezpieczenia dowodów oraz poinformowania o zdarzaniu odpowiednich osób.
1) ASI powiadamia niezwłocznie:
a) Burmistrza Sokółki o fakcie i treści zgłoszenia, 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 niniejszego planu ;
b) Inspektora Ochrony Danych, na właściwy adres poczty elektronicznej oraz telefonicznie. 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.

8. Wykaz incydentów w podziale a 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
	Nieskwalifikowane
Próby włamań	Wykorzystanie znanych luk systemowych
	Próby nieudanego logowania

	Wykorzystanie nieznanych luk systemowych
	Nieskwalifikowane
Włamania	Włamanie na konto uprzywilejowane
	Włamanie na konto zwykłe
	Włamanie do aplikacji
	Bot
	Nieskwalifikowane
Dostępność zasobów	Atak blokujący serwis (DoS)
	Rozproszony atak blokujący serwis (DDoS)
	Sabotaż komputerowy
	Przerwa w działaniu usług (niezłośliwe)
	Nieskwalifikowane
Atak na bezpieczeństwo informacji	Nieuprawniony dostęp do informacji
	Nieuprawniona zmiana informacji
	Nieskwalifikowane
Oszustwa komputerowe	Nieuprawnione wykorzystanie zasobów
	Naruszenie praw autorskich
	Kradzież tożsamości, podszycie się
	Phishing
	Nieskwalifikowane
Podatne usługi	Otwarte serwisy podatne na nadużycia
	Nieskwalifikowane
inne	...

9. Formularz zgłoszenia incydentu

FORMULARZ ZGŁOSZENIA INCYDENTU	
Imię i nazwisko	
Stanowisko służbowe	
Kontakt (nr telefonu, e-mail)	
Czy incydent miał/ ma wpływ na realizację zadań publicznych? Jeśli tak, na jakie?	
Dokładna lub przybliżona liczba osób, na które ma wpływ incydent	
Moment wystąpienia i wykrycia incydentu oraz przybliżony czas jego trwania	
Zasięg geograficzny obszaru, którego dotyczy incydent	
Skutki oddziaływania incydentu na systemy informacyjne w Podmiocie	
Informacje o przyczynie i źródle incydentu	
Opis przebiegu incydentu (najdokładniej jak to możliwe)	
Informacje o podjętych działaniach zapobiegawczych	
Informacje o podjętych działaniach naprawczych	
Inne istotne informacje	