ZARZĄDZENIE NR 0050.81.2022
WÓJTA GMINY LUBICZ

z dnia 26 września 2022 r.

w sprawie wprowadzenia w Urzędzie Gminy Lubicz procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem

Na podstawie art. 30 ust. 1 i art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2021 r. poz. 1372 z późn. zm.) w zw. z art. 21 ust. 1 i art. 22 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz. UL z 2020 r. poz. 1369 z późn. zm.) oraz § 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 (Dz. U. z 2017 r. poz. 2247 z późn. zm.) zarządza się, co następuje:

1. Wprowadza się do użytku służbowego w Urzędzie Gminy Lubicz procedurę zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem, stanowiącą Załącznik Nr 1 do niniejszego zarządzenia.

2. Zobowiązuje się wszystkich pracowników Urzędu Gminy Lubicz do zapoznania się z Procedurą, o której mowa w § 1.

3. Pisemne oświadczenie o zapoznaniu się i przestrzeganiu postanowień Procedury, stanowiące Załącznik Nr 2 do niniejszego zarządzenia, należy złożyć na stanowisku ds. kadrowych Urzędu Gminy Lubicz.

4. Zarządzenie wchodzi w życie z dniem popisania.

Wójt Gminy Lubicz

Marek Nicewicz

Załącznik do zarządzenia Nr 0050.81.2022
Wójta Gminy Lubicz
z dnia 26 września 2022 r.

PROCEDURA ZARZĄDZANIA INCYDENTAMI BEZPIECZEŃSTWA

Spis treści

Wstęp

Cel i zadania

1) Celem niniejszej Procedury jest zapewnienie, by zdarzenia (incydenty) związane z zagrożeniem bezpieczeństwa systemu informatycznego w Urzędzie Gminy Lubicz były zgłaszane Administratorowi, Informatykowi w sposób umożliwiający szybkie reagowanie, podjęcie działań zaradczych, jak również realizację obowiązków notyfikacyjnych względem organu nadzorczego oraz osób, których dotyczą.
2) Niniejsza procedura reguluje postępowanie pracowników Urzędu Gminy Lubicz w zakresie prawidłowego reagowania w przypadku stwierdzenia wystąpienia incydentu bezpieczeństwa systemu informatycznego..

Słownik pojęć

1) **Integralność** – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany, nie są zagrożone nieautoryzowaną manipulacją, celową lub przypadkową.
2) **Poufność** – właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom.
3) **Dostępność** – możliwość wykorzystania danych na żądanie, w założonym czasie przez kogoś lub coś, kto lub co ma do tego prawo.
4) **Zdarzenie** – pojedyncze zdarzenie związane z bezpieczeństwem systemów informatycznych lub serię takich zdarzeń, które może (ale nie musi) stwarzać prawdopodobieństwo naruszenia ich ochrony.
5) **Incydent** – pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji, czyli zachowaniu poufności, integralności i dostępności.

3. Klasyfikacja incydentów

1) Incydentem może być:
   - zgubienie lub kradzież nośnika /urządzenia na którym znajdują się dane służbowe,
   - nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń,
   - złośliwe oprogramowanie integrujące w poufność, integralność lub dostępność danych,
   - uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy,
   - nieprawidłowe usunięcie/zniszczenie z nośnika urządzenia danych,
   - przypadkowe usunięcie istotnych danych przez administratora aplikacji,
   - atak na jeden z systemów znajdujących się w Urzędzie Gminy Lubicz,
   - brak zasilania elektrycznego skutkujący niedostępnością istotnej infrastruktury IT,
   - nieprzestrzeganie obowiązujących procedur bezpieczeństwa lub obowiązującego prawa (np. ustawy o ochronie danych osobowych),
   - wyciek istotnych danych z Urzędu Gminy Lubicz,
   - zalanie pomieszczeń serwerowych,
   - rażące naruszenie dyscypliny pracy w zakresie przestrzegania Polityki Bezpieczeństwa Informacji poprzez: niewylogowanie się, pozostawienie włączonego komputera po zakończeniu pracy, niezamknięcie pokoju itp.
2) Incydenty można sklasyfikować w następujący sposób:
   - Zdarzenia losowe zewnętrzne – np. klęski żywiołowe, przerwy w zasilaniu,
   - Zdarzenia losowe wewnętrzne – np. zamierzone/niezamierzone pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu,
   - Zdarzenia zamierzone, świadome i celowe – np. nieuprawiony dostęp do danych z zewnątrz (włamanie do systemu), nieuprawiony dostęp do danych z sieci wewnętrznej, nieuprawiony transfer danych, pogorszenie działania sprzętu lub oprogramowania (działanie wirusów), kradzież sprzętu.

4. Wykrywanie i obsługa incydentów IT

Na Obsługę incydentu składa się:

Wykrycie incydentu,

Potwierdzenie oraz jego wstępna analiza,

Ograniczenie wpływu incydentu na infrastrukturę IT,

Usunięcie skutków incydentu

Odpowiedź na incydent.

4.1. Wykrycie incydentu

Incydenty mogą być wykrywane na kilka sposobów:

- automatyczne zgłoszenie przez jeden z systemów (np. IDS, antywirus),
- zgłoszenie przez osobę niebędącą pracownikiem Urzędu Gminy Lubicz,
- zgłoszenie przez pracownika Urzędu Gminy Lubicz,
- zgłoszenie przez pracownika technicznego (np. administratora, osobę analizującą okresowo logi systemowe).

W przypadku stwierdzenia lub podejrzenia, że doszło lub może dojść do naruszenia bezpieczeństwa systemu teleinformatycznego pracownik ma obowiązek niezwłocznie dokonać zgłoszenia tego faktu mailem na adres email inspektora ochrony danych/informatyka

Każde zgłoszenie musi zawierać:

- imię i nazwisko zgłaszającego, komórkę organizacyjną oraz stanowisko/funkcję, dane kontaktowe,
- miejsce i datę wystąpienia incydentu,
- informacje o systemie lub urządzeniu, którego dotyczy incydent,
- opis zdarzenia.

Osoba zgłaszająca incydent nie powinna podejmować samodzielnie żadnych działań (na własną rękę) oraz w miarę możliwości zabezpieczyć materiał dowodowy np. poprzez wykonanie zdjęć ekranu komputera, zrobienie zrzutu ekranu itp.

W przypadku wystąpienia incydentu fakt ten zgłasza się odpowiednio:

- informatykowi,
- Administratorowi – Wójtowi Gminy Lubicz,
- Inspektorowi Danych Osobowych - zakresie ochrony danych osobowych,
- Bezpośredniemu przełożonemu.

Informatyk prowadzi *Rejestr zgłoszeń związanych z bezpieczeństwem systemów teleinformatycznych*, w którym odnotowuje wszystkie zdarzenia, które zostały mu zgłoszone. Rejestr jest prowadzony w wersji elektronicznej. Wzór rejestru stanowi załącznik do procedury.

Potwierdzenie oraz analiza incydentu

Potwierdzenie incydentu (w niektórych przypadkach zgłaszany incydent nie jest incydentem tylko zdarzeniem). Analiza zgłoszenia powinna obejmować:

- określenie krytyczności problemu (priorytetu incydentu),
- określenie ewentualnego wpływu na inne systemy oraz jego rozległość,
- wpływ incydentu na ciągłość działania ,
- wrażliwość informacji, których poufność dostępność lub integralność naruszono,
- rozmiar szkód powstałych skutkiem incydentu,
- koszt usunięcia i naprawy skutków incydentu,
- szacowany czas przywrócenia ciągłości działania systemu dotkniętego incydentem,
- zasoby wymagane do przywrócenia ciągłości działania systemu.

Dodatkowo dla incydentu określany jest również priorytet incydentu. Określenie stopnia krytyczności incydentu określa poniższa tabela.

WPŁYW NA ZASÓB	KRYTYCZNOŚĆ ZASOBU		
	niska	**średnia**	**wysoka**
Wysoki	średni	wysoki	wysoki
Średni	niski	średni	wysoki
Niski	niski	niski	średni

Priorytet incydentu determinuje czas jego obsługi:

PRIORYTET INCYDENTU	CZAS NA PODJĘCIE DZIAŁAŃ NAD INCYDENTEM	MAKSYMALNY CZAS OBSŁUGI INCYDENTU
Niski	do 48h	do 21 dni
Średni	do 24h	do 7 dni
Wysoki	do 5h	do 3 dni

Potwierdzenie wystąpienia incydentu należy odnotować w ewidencji incydentów.

4.2. Obowiązek zgłoszenia do organu nadzorczego

W przypadku wystąpienia incydentu bezpieczeństwa o najwyższym priorytecie bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 48 godzin - po stwierdzeniu naruszenia bezpieczeństwa systemu IT zgłasza się ten fakt do :

1. Bezpośredniego przełożonego, który powiadamia Wójta Gminy Lubicz
2. Osoby wyznaczonej do zgłaszania incydentów do CRIST

4.3. Ograniczenie wpływu incydentu na inne systemy

Po analizie incydentu należy ograniczyć jego wpływ na inne systemy.

Przykładowe sposoby ograniczania wpływu incydentu na inne systemy:

- rekonfiguracja systemu (np. zablokowanie portu, przez który następuje wyciek danych z LAN, usunięcie niewykorzystywanej usługi systemu operacyjnego, która jest często atakowana),
- usunięcie zasadniczej przyczyny problemu (np. usunięcie malware z zainfekowanej stacji PC),
- wyłączenie systemu,
- fizyczne odcięcie systemu od sieci.

4.4. Usunięcie skutków incydentu oraz zebranie dowodów

Podstawowym celem usunięcia skutków incydentu jest przywrócenie stanu bezpieczeństwa infrastruktury IT oraz danych do stanu sprzed incydentu. Usunięcie skutków incydentu może zostać przeprowadzone na wiele różnych sposobów w zależności od konkretnego incydentu (może to być np. rekonfiguracja firewalla, wgranie odpowiednich poprawek do systemu czy wprowadzenie dodatkowych metod ochrony dla wybranych danych). Przy usuwaniu skutków incydentu należy pamiętać, aby nie zniszczyć ewentualnych dowodów wystąpienia incydentów. Zebranie dowodów polega na analizie istoty problemu jak: kto lub co było przyczyną incydentu, potwierdzenie dokładnej daty wystąpienia incydentu.

4.5. Odpowiedź na incydent

Odpowiedź na incydent może być realizowana w dwóch niezależnych trybach:

1) reakcja wewnętrzna – np.: rekonfiguracja systemów, uzupełnienie procedur, eskalacja problemu w strukturze organizacyjnej firmy, wyciągnięcie konsekwencji personalnych, implementacja wniosków na przyszłość,
2) reakcja zewnętrzna – np.: kontakt z właścicielem systemu, z którego nastąpił atak, powiadomienie policji, prokuratury, mediów.

Odpowiedź powinna być zawsze dostosowana do konkretnego incydentu oraz stopnia jego priorytetu.

5. Prowadzenie ewidencji incydentów

Każdy incydent powinien być odnotowywany jako osobna pozycja w ewidencji incydentów. Tabela taka powinna zawierać poniższe dane:

- datę wykrycia incydentu,
- status (w trakcie wyjaśniania, zamknięty, odrzucony jako nieprawdziwy),
- datę rozwiązania incydentu,
- opis incydentu,
- podjęte działania,
- zalecenia na przyszłość.

Okresowo – np. raz na pół roku - należy analizować ewidencję incydentów oraz wyciągać odpowiednie wnioski prewencyjne – tj. ograniczające liczbę incydentów w przyszłości.

Załącznik nr 1	Raport z obsługi zgłoszonego zagrożenia z systemu antywirusowego
Załącznik nr 2	Ewidencja incydentów
Załącznik nr 3	Rejestr zgłoszeń związanych z bezpieczeństwem systemów teleinformatycznych

Załącznik nr 1. Raport z obsługi zgłoszonego zagrożenia z systemu antywirusowego

Raport	
NAZWA STACJI ROBOCZEJ KTÓREJ DOTYCZY ZGŁOSZENIE:	
CZY ZAGROŻENIE ZOSTAŁO USUNIĘTE?	
WYKRYTE ZAGROŻENIA NA STACJI:	
WYNIK SKANOWANIA:	

KLASYFIKACJA: ☐ ZDARZENIE ☐ INCYDENT

FORMA DALSZYCH CZYNNOŚCI: ☐ ZAKOŃCZENIE ☐ KONTYNUACJA

Wykonał:		Akceptował:		Zatwierdził:	

Załącznik nr 2 Ewidencja incydentów

EWIDENCJA INCYDENTÓW

Lp	Data wykrycia incydentu	Opis incydentu	Podjęte działania	Status[1]	Data rozwiązania incydentu	Zalecenia na przyszłości
1						
2						
3						
4						
5						

Załącznik nr 3 Rejestr zgłoszeń związanych z bezpieczeństwem systemów teleinformatycznych

REJESTR ZGŁOSZEŃ ZWIĄZANYCH Z BEZPIECZEŃSTWEM SYSTEMÓW TELEINFORMATYCZNYCH

Lp.	Data zgłoszenia	Opis zgłoszenia	Osoba zgłaszająca	Incydent	Data rozwiązania incydentu	Zalecenia na przyszłości
1				TAK/NIE		
2				TAK/NIE		
3				TAK/NIE		
4				TAK/NIE		
5				TAK/NIE		