Warszawa, dnia 29 października 2021 r.

Poz. 27

ZARZĄDZENIE NR 27/21
SZEFA CENTRALNEGO BIURA ANTYKORUPCYJNEGO

z dnia 28 października 2021 r.

w sprawie reagowania na incydenty komputerowe w Centralnym Biurze Antykorupcyjnym

Na podstawie art. 10 ust. 3 w zw. z art. 11 ust. 4 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2021 r. poz. 1671) zarządza się, co następuje:

Rozdział 1.
Przepisy ogólne

§ 1. Zarządzenie określa:

1) zakres zadań, organizację i skład oraz zasady funkcjonowania Zespołu Reagowania na Incydenty Komputerowe, zwanego dalej „CSIRT CBA”;

2) tryb współdziałania CSIRT CBA z innymi jednostkami typu CSIRT lub CERT;

3) sposób zgłaszania incydentów i podatności, o których mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369), zwanej dalej „ustawą”.

§ 2. Użyte w zarządzeniu określenia oznaczają:

1) system informacyjny CBA - zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2021 r. poz. 576) wraz z przetwarzanymi w nim danymi w postaci elektronicznej, a także sieć teleinformatyczną, których właścicielem jest Centralne Biuro Antykorupcyjne, zwane dalej "CBA";

2) pełnomocnik - pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni Centralnego Biura Antykorupcyjnego, powoływany decyzją Szefa Centralnego Biura Antykorupcyjnego.

Rozdział 2.
Zakres zadań CSIRT CBA

§ 3. 1. CSIRT CBA jest wewnętrznym zespołem o charakterze stałym, realizującym zadania z obszaru zarządzania incydentami oraz podwyższania bezpieczeństwa jawnych systemów informacyjnych CBA.

2. Do zadań CSIRT CBA należy w szczególności:

1) zarządzanie incydentami;

2) szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, w tym prowadzenie dynamicznej analizy ryzyka;

3) współpraca z właściwymi jednostkami organizacyjnymi CBA w zakresie pozyskiwania danych niezbędnych do obsługi incydentów;

4) wykonywanie audytów i testów bezpieczeństwa jawnych systemów informacyjnych CBA;

5) opracowywanie i wydawanie zaleceń do wdrożenia w konfiguracji urządzeń oraz oprogramowania funkcjonującego w jawnych systemach informacyjnych CBA, w tym niezbędnych do usunięcia stwierdzonych podatności;

6) monitorowanie dostępnych źródeł w celu pozyskiwania wiedzy na temat pojawiających się nowych zagrożeń i podatności jawnych systemów informacyjnych CBA;

7) opracowywanie i wydawanie dobrych praktyk oraz rekomendacji w zakresie cyberbezpieczeństwa;

8) współpraca w zakresie wykrywania i wyjaśniania incydentów z innymi instytucjami, w szczególności z Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego działającym na poziomie krajowym, prowadzonym przez Szefa Agencji Bezpieczeństwa Wewnętrznego, zwanym dalej „CSIRT GOV”;

9) publikacja powiadomień oraz ostrzeżeń z zakresu cyberbezpieczeństwa, realizowana w szczególności za pośrednictwem portalu wewnętrznego CBA, usługi przesyłania krótkich wiadomości tekstowych, poczty elektronicznej lub innych kanałów komunikacyjnych;

10) prowadzenie szkoleń z zakresu cyberbezpieczeństwa dla funkcjonariuszy oraz pracowników CBA;

11) budowa, utrzymywanie i rozwijanie środowiska testowego, przeznaczonego do analizy złośliwego oprogramowania i podatności;

12) udział w prowadzonych przez pełnomocnika pracach związanych z opracowywaniem i wydawaniem procedur reagowania na incydenty w CBA;

13) przyjmowanie zgłoszeń wystąpienia lub podejrzenia wystąpienia incydentów lub podatności od funkcjonariuszy i pracowników CBA;

14) wyjaśnianie incydentów i podatności zgłoszonych w ramach współpracy z zewnętrznymi jednostkami typu CSIRT lub CERT;

15) udzielanie niezbędnej pomocy pełnomocnikowi do spraw ochrony informacji niejawnych, pełnomocnikowi do spraw kontroli przetwarzania przez CBA danych osobowych, kierownikom jednostek organizacyjnych, rzecznikom dyscyplinarnym, zespołom kontrolnym oraz innym osobom i zespołom, w przypadku prowadzenia przez nich postępowań związanych z wystąpieniem incydentu;

16) prowadzenie witryny intranetowej na portalu wewnętrznym CBA oraz publikowanie na tej witrynie biuletynów informacyjnych oraz zaleceń i wytycznych.

3. Zalecenia wydawane przez CSIRT CBA, z wyłączeniem zaleceń, o których mowa w ust. 1 pkt 5, są uzgadniane z pełnomocnikiem.

4. CSIRT CBA uwzględnia zalecenia pełnomocnika, a także udziela mu informacji oraz przygotowuje raporty z pracy CSIRT CBA na jego wniosek.

Rozdział 3.
Organizacja i skład CSIRT CBA

§ 4. 1. CSIRT CBA kieruje naczelnik Wydziału III Departamentu Bezpieczeństwa CBA, zwany dalej „kierownikiem CSIRT CBA”.

2. W skład CSIRT CBA wchodzą funkcjonariusze Wydziału III Departamentu Bezpieczeństwa CBA wyznaczeni przez dyrektora Departamentu Bezpieczeństwa CBA.

3. W uzasadnionych przypadkach, kierownik CSIRT CBA może występować do właściwych kierowników jednostek organizacyjnych CBA o włączenie do prac CSIRT CBA funkcjonariuszy

z kierowanych przez nich jednostek organizacyjnych oraz o udzielenie pomocy poprzez użyczenie urządzeń lub systemów informacyjnych CBA.

Rozdział 4.
Zasady funkcjonowania CSIRT CBA

§ 5. 1. Za realizację zadań CSIRT CBA odpowiada kierownik CSIRT CBA.

2. Do zadań kierownika CSIRT CBA należy:

1) organizowanie pracy CSIRT CBA;

2) określanie aktualnych kierunków działań CSIRT CBA oraz ustalanie ich priorytetów;

3) zlecanie zadań poszczególnym członkom CSIRT CBA;

4) przedstawianie na wniosek pełnomocnika informacji i raportów z pracy CSIRT CBA;

5) organizowanie współpracy z zewnętrznymi jednostkami typu CSIRT lub CERT, w szczególności z CSIRT GOV;

6) reprezentowanie CBA w kontaktach z CSIRT GOV.

3. Kierownik CSIRT CBA, we współdziałaniu z właściwymi kierownikami jednostek organizacyjnych, implementuje oraz stosuje środki techniczne i organizacyjne, a także narzędzia do kontroli konfiguracji systemów informacyjnych CBA oraz służące do zapobiegania incydentom i ich wykrywania.

4. W przypadku wykrycia incydentu lub podatności, kierownik CSIRT CBA może wnioskować do kierownika jednostki organizacyjnej odpowiedzialnego za system informacyjny CBA o czasowe wyłączenie, ograniczenie funkcjonalności lub zaniechanie przetwarzania informacji w tym systemie lub jego części.

§ 6. Do obowiązków członków CSIRT CBA należy wykonywanie zadań zleconych przez kierownika CSIRT CBA.

§ 7. Nadzór nad funkcjonowaniem CSIRT CBA sprawuje pełnomocnik.

Rozdział 5.
Współpraca z innymi jednostkami typu CSIRT lub CERT

§ 8. 1. Współpracę z zewnętrznymi jednostkami typu CSIRT lub CERT, w szczególności z CSIRT GOV, mogą podejmować funkcjonariusze wchodzący w skład CSIRT CBA.

2. Przekazanie urządzeń i nośników wykorzystywanych w jawnych systemach informacyjnych CBA, wnioskowane przez podmioty uprawnione w związku z prowadzonymi wyjaśnieniami incydentów, możliwe jest wyłącznie za zgodą pełnomocnika.

Rozdział 6.
Sposób zgłaszania incydentów i podatności

§ 9. 1. Funkcjonariusz lub pracownik CBA zgłasza wystąpienie lub podejrzenie wystąpienia incydentu lub podatności co najmniej jednej z następujących grup funkcjonariuszy lub pracowników:

1) CSIRT CBA;

2) Sekcji Cyberbezpieczeństwa Biura Teleinformatycznego CBA;

3) Help Desk Biura Teleinformatycznego CBA.

2. Funkcjonariusze lub pracownicy, o których mowa w ust. 1 pkt 2 i 3, niezwłocznie powiadamiają funkcjonariuszy CSIRT CBA o otrzymaniu zgłoszenia o incydencie lub podatności oraz o wystąpieniu lub podejrzeniu wystąpienia incydentu lub podatności.

3. CSIRT CBA może kierować zapytania uzupełniające do osób, które dokonały zgłoszenia.

4. Szczegółowe dane kontaktowe lub inne wytyczne w zakresie zgłaszania incydentów i podatności określa pełnomocnik.

Rozdział 7.
Przepisy końcowe

§ 10. Zarządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

Szef Centralnego Biura Antykorupcyjnego

Andrzej Stróżny