Zarządzenie Nr 80/2022

Burmistrza Biskupca

z dnia 22 lutego 2022 roku

w sprawie zmiany stopnia alarmowego CRP na terenie Gminy Biskupiec

Na postawie art. 16 ust. 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2021 r., poz. 2234), Rozporządzenia Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (Dz. U. z 2016 r., poz. 1101) oraz Zarządzenia Nr 425 Burmistrza Biskupca z dnia 8 grudnia 2017 roku w sprawie ustalenia procedur postępowania w stanach gotowości obronnej Państwa po wprowadzeniu poszczególnych stopni alarmowych i stopni alarmów CRP, zarządza się, co następuje:

§ 1. Zmienia się, wprowadzony zarządzeniem nr 77/2022 Burmistrza Biskupca z dnia 16 lutego 2022 r. w sprawie wprowadzenia pierwszego stopnia alarmowego na terenie Gminy Biskupiec, stopień alarmowy CRP, przez wprowadzenie na terenie Gminy Biskupiec trzeciego stopnia alarmowego CRP (stopnia CHARLIE-CRP), obowiązującego od dnia 21 lutego 2022 r., od godz. 21:00, do dnia 4 marca 2022 r., do godz. 23:59, w miejsce pierwszego stopnia alarmowego CRP (stopnia ALFA-CRP) obowiązującego na terenie Gminy Biskupiec, od dnia 15 lutego 2022 r., od godz. 23:59, do dnia 28 lutego 2022 r., do godz. 23:59.

§ 2. Zalecenia dotyczące postępowania po wprowadzeniu stopnia alarmowego stanowią załącznik do niniejszego Zarządzenia.

§ 3. Wprowadza się całodobowe dyżury administratora systemów teleinformatycznych w Urzędzie Miejskim w Biskupcu. W tym celu wyznacza się pracowników:

1) Piotr Lipka,
2) Bartosz Turonek,
3) Marek Wiśniewski,
4) Mirosław Wołyniec.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
mgr Kamil Kozłowski

Załącznik do Zarządzenia Nr 80/2022
Burmistrza Biskupca
z dnia 22 lutego 2022 roku

Po wprowadzeniu trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP) należy wykonać zadania wymienione dla pierwszego i drugiego stopnia alarmowego CRP oraz kontynuować lub sprawdzić wykonanie tych zadań, jeżeli wcześniej był wprowadzony stopień ALFA-CRP lub BRAVO-CRP.

I. Przedsięwzięcia realizowane w ramach trzeciego stopnia alarmowego CRP

1) wprowadzenie całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów;

2) dokonanie przeglądu dostępnych zasobów zapasowych pod względem możliwości ich wykorzystania w przypadku zaistnienia ataku;

3) przygotowanie się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku, w tym:

a) dokonanie przeglądu i ewentualnego audytu planów awaryjnych oraz systemów,

b) przygotowanie się do ograniczenia operacji na serwerach, w celu możliwości ich szybkiego i bezawaryjnego zamknięcia.

II. Przedsięwzięcia realizowane w ramach II stopnia BRAVO – CRP:

1) zapewnienie dostępności w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów;

2) wprowadzenie całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych.

III. Przedsięwzięcia realizowane w ramach pierwszego stopnia alarmowego CRP (stopień ALFA-CRP):

1) poinformowanie personelu instytucji, w szczególności odpowiedzialnych za bezpieczeństwo systemów teleinformatycznych, o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy;
2) zapewnienie dostępu w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów teleinformatycznych;
3) sprawdzenie kanałów łączności z innymi podmiotami biorącymi udział w reagowaniu kryzysowym właściwymi dla rodzaju stopnia alarmowego CRP, zespołami reagowania na

incydenty bezpieczeństwa teleinformatycznego właściwymi dla rodzaju działania organizacji oraz ministrem właściwym do spraw informatyzacji;

4) dokonanie przeglądu stosownych procedur oraz zadań związanych z wprowadzeniem stopni alarmowych CRP;
5) sprawdzenie aktualnego stanu bezpieczeństwa infrastruktury teleinformatycznej i ocena wpływu zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń;
6) informowanie na bieżąco o efektach przeprowadzanych działań zespoły reagowania na incydenty bezpieczeństwa teleinformatycznego właściwe dla rodzaju działania organizacji oraz współdziałające centra zarządzania kryzysowego, a także ministra właściwego do spraw informatyzacji.