

Procedury postępowania dla administratora przy zagrożeniu atakiem terrorystycznym

Zgodnie z art. 23 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t. j. Dz. U.z 2013 r., poz. 1166 ze zm.) oraz Zarządzenia nr 18 Prezesa Rady Ministrów z dnia 2 marca 2016 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego, w zależności od skali zagrożenia atakiem o charakterze terrorystycznym lub sabotażowym, Prezes Rady Ministrów, ministrowie i kierownicy urzędu centralnego oraz wojewodowie, w drodze zarządzenia, mogą wprowadzić następujące stopnie alarmowe:

<static/img/k02/ZKR/Stopnie%20alarmowe%20-%20tabela%20.pdf>

Przedsięwzięcia realizowane w ramach I stopnia alarmowego (stopień ALFA):

Na rzecz ochrony ludności:

1. Prowadzić wzmożoną kontrolę miejsc dużych skupisk ludzkich, obiektów użyteczności publicznej oraz innych potencjalnych obiektów ataku, w celu wzmocnienia ochrony.
2. Informować odpowiednie służby w przypadku zauważenia: nieznanymi pojazdami na terenie instytucji publicznych lub innych ważnych obiektów, porzuconych paczek i bagaży lub w przypadku zaobserwowania jakichkolwiek innych oznak nietypowej działalności.

Na rzecz ochrony infrastruktury:

1. Informować podległy personel o konieczności zachowania wzmożonej czujności w stosunku do osób, zachowujących się w sposób wzbudzający podejrzenia.
2. Zapewnić dostępność w trybie alarmowym członków personelu niezbędnego do wzmocnienia ochrony obiektów.
3. Przeprowadzać kontrole pojazdów wjeżdżających oraz osób wchodzących na teren obiektów.
4. Sprawdzać na zewnątrz i od zewnątrz budynki będące w stałym użyciu, pod względem podejrzanych zachowań osób oraz w poszukiwaniu podejrzanych przedmiotów.
5. Sprawdzić działanie środków łączności wykorzystywanych w celu zapewnienia bezpieczeństwa.
6. Dokonać przeglądu wszystkich procedur, rozkazów, szczegółowych wymagań osobowych i logistycznych oraz zadań związanych z wprowadzeniem wyższych stopni alarmowych.
7. Sprawdzić działanie instalacji alarmowych oraz przepustowość dróg ewakuacji.

Przedsięwzięcia realizowane w ramach II stopnia alarmowego (stopień BRAVO):

Na rzecz ochrony ludności:

1. Wprowadzić dodatkowe kontrole pojazdów, ludzi oraz budynków publicznych w rejonach zagrożonych.
2. Rozszerzyć akcję informacyjno-instruktażową dla społeczeństwa dotyczącą potencjalnego zagrożenia, jego skutków i sposobu postępowania.

Na rzecz ochrony infrastruktury:

1. Ostrzec personel o możliwych formach ataku.
2. Zapewnić dostępność w trybie alarmowym personelu wyznaczonego do wdrażania procedur działania na wypadek ataków terrorystycznych i sabotażowych.
3. Sprawdzić i wzmocnić ochronę ważnych obiektów publicznych.
4. Sprawdzić systemy ochrony obiektów ochraniających przez specjalistyczne uzbrojone formacje ochronne i wewnętrzne służby ochrony.
5. Wprowadzić kontrole wszystkich przesyłek pocztowych i kurierskich kierowanych do urzędu (instytucji).
6. Zamknąć i zabezpieczyć nieużywane regularnie budynki i pomieszczenia.
7. Dokonać przeglądu posiadanych zapasów materiałowych i sprzętu.
8. Zapewnić ochronę środków transportu służbowego poza terenem obiektu, wprowadzić kontrolę pojazdu przed wejściem do samochodu i jego uruchomieniem.

Przedsięwzięcia realizowane w ramach III stopnia alarmowego (stopień CHARLIE):**Na rzecz ochrony ludności:**

1. Wzmocnić ochronę organizowanych imprez masowych wg decyzji organu wydającego zezwolenie na przeprowadzenie imprezy masowej lub odwołać organizację imprez, jeżeli nie ma możliwości wzmocnienia ochrony lub wzmocnienie nie gwarantuje zapobieżenia ewentualnemu atakowi.
2. Wzmocnić ochronę organizowanych zgromadzeń publicznych lub znaleźć organizatora w celu odwołania planowanych zgromadzeń publicznych.
3. Dokonać przeglądu dostępnej infrastruktury, zasobów i środków medycznych pod kątem możliwości wykorzystania w przypadku ataku terrorystycznego lub sabotażowego.
4. Zweryfikować dane o obiektach wyznaczonych na zastępcze miejsca czasowego pobytu na wypadek ewakuacji ludzi.

Na rzecz ochrony infrastruktury:

1. Wprowadzić dyżury dla osób funkcyjnych odpowiedzialnych za wprowadzanie procedur działania na wypadek aktów terrorystycznych lub sabotażowych.
2. Ograniczyć do minimum liczbę miejsc ogólnodostępnych w obiekcie i rejonie obiektu,
3. Wprowadzić w uzasadnionych wypadkach ścisłą kontrolę osób i pojazdów przy wejściu i wjeździe na teren obiektów.
4. Ograniczyć możliwości parkowania pojazdów przy obiektach chronionych.
5. Wydać broń i amunicję oraz środki ochrony osobistej uprawnionym osobom wyznaczonym do wykonywania zadań ochronnych.
6. Wprowadzić dodatkowy całodobowy nadzór miejsc, które tego wymagają, do tej pory nieobjętych nadzorem.
7. Wdrożyć dodatkowe procedury bezpieczeństwa w placówkach dyplomatycznych i urzędach konsularnych poza granicami kraju wynikające z planów ochrony.

Przedsięwzięcia realizowane w ramach IV stopnia alarmowego (stopień DELTA):**Na rzecz ochrony ludności:**

1. Wprowadzić w uzasadnionych przypadkach ograniczenia komunikacyjne w rejonach zagrożonych.
2. Wprowadzić w uzasadnionych przypadkach zakaz przeprowadzania imprez masowych i zgromadzeń publicznych.

Na rzecz ochrony infrastruktury:

1. Przeprowadzić identyfikację wszystkich pojazdów znajdujących się już w rejonie obiektu oraz w uzasadnionych przypadkach ich relokację poza obszar obiektu.
2. Kontrolować wszystkie pojazdy wjeżdżające na teren obiektu i ich ładunek.
3. Kontrolować wszystkie wnoszone na teren obiektu przedmioty w tym walizki, torebki i paczki.
4. Przeprowadzać częste kontrole na zewnątrz budynku i na parkingach.
5. Ograniczyć liczbę podróży służbowych osób zatrudnionych w obiekcie i wizyt osób niezatrudnionych w instytucji.
6. Przygotować się do zapewnienia ciągłości funkcjonowania organów w przypadku braku możliwości realizacji zadań w dotychczasowym miejscu pracy.

Stopnie alarmowe CRP**Przedsięwzięcia realizowane w ramach I stopnia alarmowego CRP (stopień ALFA-CRP):**

Po wprowadzeniu I stopnia alarmowego CRP (stopień ALFA-CRP) należy wykonać w szczególności następujące zadania:

1. Poinformować personel, w szczególności odpowiadający za bezpieczeństwo systemów teleinformatycznych, o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy.
2. Zapewnić dostępność w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów teleinformatycznych.
3. Sprawdzić kanały 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. Dokonać przeglądu stosowanych procedur oraz zadań związanych z wprowadzeniem stopni alarmowych CRP.

5. Sprawdzić aktualny stan bezpieczeństwa infrastruktury teleinformatycznej i ocenić wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń.

6. Informować 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.

Przedsięwzięcia realizowane w ramach II stopnia alarmowego CRP (stopień BRAVO-CRP):

Po wprowadzeniu II stopnia alarmowego CRP (stopień BRAVO-CRP) należy wykonać zadania wymienione dla pierwszego stopnia alarmowego CRP oraz kontynuować lub sprawdzić wykonanie tych zadań, jeśli wcześniej był wprowadzony stopień ALFA-CRP. Ponadto należy wykonywać w szczególności następujące zadania:

1. Zapewnić gotowość do niezwłocznego podejmowania działań przez administratorów systemów kluczowych dla funkcjonowania organizacji.

2. Wprowadzić dyżury w trybie alarmowym osobom uprawnionym do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych.

3. Wprowadzić wzmożone monitorowanie stanów bezpieczeństwa systemów teleinformatycznych, w tym w szczególności wykorzystując zalecenia szefa ABW lub komórek odpowiedzialnych za system reagowania, zgodnie z właściwością oraz:

a) monitorować i weryfikować czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej,

b) sprawdzać dostępność usług elektronicznych,

c) w razie potrzeby dokonywać zmian w dostępie do infrastruktury teleinformatycznej.

Przedsięwzięcia realizowane w ramach III stopnia alarmowego CRP (stopień CHARLIE-CRP):

Po wprowadzeniu III stopnia alarmowego CRP (stopień CHARLIE-CRP) należy wykonać zadania wymienione dla pierwszego i drugiego stopnia alarmowego CRP oraz kontynuować lub sprawdzić wykonanie tych zadań, jeśli wcześniej był wprowadzony stopień ALFA-CRP lub BRAVO-CRP. Ponadto należy wykonywać w szczególności następujące zadania:

1. Dokonać przeglądu dostępnych przeglądów zapasowych pod względem możliwości ich wykorzystania w wypadku zaistnienia ataku.

2. Przygotować się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku w tym m.in.:

a) dokonać przeglądu i ewentualnego audytu planów awaryjnych oraz infrastruktury teleinformatycznej,

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

Przedsięwzięcia realizowane w ramach IV stopnia alarmowego CRP (stopień DELTA-CRP):

Po wprowadzeniu IV stopnia alarmowego CRP (stopień DELTA-CRP) należy wykonać zadania wymienione dla pierwszego, drugiego i trzeciego stopnia alarmowego CRP oraz kontynuować lub sprawdzić wykonanie tych zadań, jeśli wcześniej był wprowadzony stopień ALFA-CRP, BRAVO-CRP lub CHARLIE-CRP. Ponadto należy wykonywać w szczególności następujące zadania:

1. Uruchomić plany awaryjne lub plany ciągłości działania organizacji w sytuacjach awarii lub utraty ciągłości działania,

2. Stosownie do sytuacji przystąpić do realizacji procedur przywracania ciągłości działania.

Po wprowadzeniu wymienionych stopni alarmowych należy niezwłocznie wykonać następujące zadania, które przedstawiają tabele w linku poniżej:

<static/img/k02/ZKR/Tabele%20zada%C5%84%20-%20po%20wprowadzeniu%20stopni%20alarmowych.pdf>