ZARZĄDZENIE NR 13/ZK/WCH/2022

Dziekana Wydziału Chemii
Uniwersytetu im. Adama Mickiewicza w Poznaniu
z dnia 1 września 2022r.
w sprawie zadań i czynności prowadzonych na terenie budynku Collegium Chemicum w związku z wprowadzeniem **drugiego stopnia alarmowego (stopień BRAVO) oraz trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP)**

Na podstawie art. 16 ust. 1 Ustawy z dnia 10 czerwca 2016r. o działaniach antyterrorystycznych (Dz. U. z 2021r. poz. 2234 oraz z 2022r. poz. 583 i 655), Prezes Rady Ministrów podpisał Zarządzenie nr 283 z dnia 30 sierpnia 2022r. w sprawie wprowadzenia stopnia alarmowego (2. stopień BRAVO) oraz Zarządzeniem 283 z dnia 30 sierpnia 2022r. w sprawie wprowadzenia stopnia alarmowego CRP (3. stopnia CHARLIE-CRP) na całym terytorium RP, obowiązujące od dnia 1 września 2022r. od godz. 00:00 do dnia 30 listopada 2022r. do godz. 23:59, **zarządzam wykonanie następujących przedsięwzięć:**

A) Kontynuować i sprawdzać wykonywanie zadań określonych dla pierwszego i drugiego stopnia alarmowego tj.:

I). Dla pierwszego stopnia alarmowego (stopień ALFA):

1. Prowadzić, w ramach realizacji zadań administratorów obiektów, wzmożoną kontrolę obiektów użyteczności publicznej oraz innych obiektów, które potencjalnie mogą stać się celem zdarzenia o charakterze terrorystycznym;
2. Zalecić podległemu personelowi informowanie odpowiednich służb w przypadku zauważenia: nieznanych pojazdów na terenie instytucji publicznych lub innych ważnych obiektów, porzuconych paczek i bagaży lub jakichkolwiek innych oznak nietypowej działalności;
3. Poinformować podległy personel o konieczności zachowania zwiększonej czujności w stosunku do osób zachowujących się w sposób wzbudzający podejrzenia;
4. Zapewnić dostępność w trybie alarmowym członków personelu niezbędnych do wzmocnienia ochrony obiektów;
5. Przeprowadzić kontrolę pojazdów wjeżdżających oraz osób wchodzących na teren obiektów;
6. Sprawdzać, na zewnątrz i od wewnątrz, budynki będące w stałym użyciu w zakresie podejrzanych zachowań osób oraz w poszukiwaniu podejrzanych przedmiotów;
7. Sprawdzić działanie środków łączności wykorzystywanych w celu zapewnienia bezpieczeństwa;
8. Dokonać, w ramach realizacji zadań administratorów obiektów, sprawdzenia działania instalacji alarmowych, przepustowości dróg ewakuacji oraz funkcjonowania systemów rejestracji obrazu;
9. Dokonać przeglądu wszystkich procedur, rozkazów oraz zadań związanych z wprowadzeniem wyższych stopni alarmowych;

10. Prowadzić akcję informacyjno-instruktażową dla społeczeństwa dotyczącą potencjalnego zagrożenia, jego skutków i sposobu postępowania.

B) Wykonać w szczególności następujące zadania:

II). Dla drugiego stopnia alarmowego (stopień BARVO):

1. Sprawdzić funkcjonowanie zasilania awaryjnego;
2. Ostrzec personel o możliwych formach zdarzenia o charakterze terrorystycznym;
3. Zapewnić dostępność w trybie alarmowym personelu wyznaczonego do wdrażania procedur działania na wypadek zdarzeń o charakterze terrorystycznym;
4. Wprowadzić zakaz wstępu do przedszkoli, szkół i uczelni osobom postronnym;
5. Zamknąć i zabezpieczyć nieużywane regularnie budynki i pomieszczenia;
6. Dokonać przeglądu zapasów materiałowych i sprzętu, w tym dostępności środków i materiałów medycznych, z uwzględnieniem możliwości wykorzystania w przypadku wystąpienia zdarzenia o charakterze terrorystycznym.

B) Kontynuować i sprawdzać wykonywanie zadań określonych dla pierwszego i drugiego stopnia alarmowego CRP tj.:

I). Dla pierwszego stopnia alarmowego CRP (stopień ALFA-CRP):

1. Wprowadzić wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, zwanych dalej „systemami", w szczególności wykorzystując zalecenia Szefa Agencji Bezpieczeństwa Wewnętrznego lub komórek odpowiedzialnych za system reagowania zgodnie z właściwością oraz:
   a) monitorować i weryfikować, czy nie doszło do naruszeń bezpieczeństwa komunikacji elektronicznej,
   b) sprawdzać dostępność usług elektronicznych,
   c) dokonać, w razie potrzeby zmian, w dostępie do systemów,
2. Poinformować personel o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności personel odpowiedzialny za bezpieczeństwo systemów;
3. Sprawdzić kanały łączności z innymi, właściwymi dla rodzaju stopnia alarmowego CRP, podmiotami biorącymi udział w reagowaniu kryzysowym, dokonać weryfikacji ustanowionych punktów kontaktowych z 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, a w szczególności dokonać weryfikacji posiadanej kopii zapasowej systemów w stosunku do systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej oraz systemów kluczowych dla funkcjonowania organizacji, oraz weryfikacji czasu wymaganego na przywrócenie poprawności funkcjonowania sytemu;
5. Sprawdzić aktualny stan bezpieczeństwa systemów i ocenić wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń;
6. Informować na bieżąco o efektach przeprowadzonych działań zespołu reagowania na incydenty bezpieczeństwa teleinformatycznego właściwe dla rodzaju działania organizacji oraz współdziałające centra zarządzania kryzysowego, a także ministra właściwego do spraw informatyzacji.

II) Dla drugiego stopnia alarmowego CRP (stopień BRAVO-CRP)

1. Zapewnić dostępność w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów;
2. Wprowadzić całodobowe dyżury administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych.

B) wykonać w szczególności następujące zadania:

III) Dla trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP)

1. Wprowadzić całodobowe dyżury administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów;
2. Dokonać przeglądu dostępnych zasobów zapasowych pod względem możliwości ich wykorzystania w przypadku zaistnienia ataku;
3. Przygotować się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku, w tym:
   a) dokonać przeglądu i ewentualnego audytu planów awaryjnych oraz systemów,
   b) przygotować się do ograniczenia operacji na serwerach, w celu możliwości ich szybkiego i bezawaryjnego zamknięcia.

DZIEKAN
Wydziału Chemii
prof. dr hab. Maciej Kubicki