

ZARZĄDZENIE NR 3/ZK/WCH/2022

Dziekana Wydziału Chemii
Uniwersytetu im. Adama Mickiewicza w Poznaniu
z dnia 22 lutego 2022r.

w sprawie zadań i czynności prowadzonych na terenie budynku Collegium
Chemicum w związku z wprowadzeniem **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), Prezes Rady Ministrów podpisał Zarządzenie nr 40 z dnia 21 lutego 2022r. w sprawie zmiany stopnia alarmowego CRP, stopień alarmowy CRP przez wprowadzenie na całym terytorium RP trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP), obowiązującego od dnia 21 lutego 2022r. od godz. 21:00 do dnia 04 marca 2022r. do godz. 23:59, w miejsce pierwszego stopnia alarmowego CRP (stopień ALFA-CRP), obowiązującego na całym terytorium RP od dnia 15 lutego od godz. 23:59 do dnia 28 lutego 2022r. do godz. 23:59, zarządzam wykonanie następujących przedsięwzięć:

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

D). 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 systemu;
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