

Zarządzenie Nr 187/2022 Prezydenta Miasta Ciechanów z dnia 1 sierpnia 2022 roku

w sprawie wprowadzenia stopnia alarmowego CHARLIE-CRP na terenie całego kraju oraz wykonania przedsięwzięć obowiązujących w Urzędzie Miasta Ciechanów i jednostkach podległych Prezydentowi Miasta.

Na podstawie Zarządzenia Nr 233 Prezesa Rady Ministrów z dnia 29 lipca 2022 roku oraz artykułu 19 ustęp 2 punkt 5 ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dziennik Ustaw z roku 2022, pozycja 261 tekst jednolity), w związku z artykułem 4 ustawy z dnia 10 czerwca 2016 roku o działaniach antyterrorystycznych (Dziennik Ustaw z 2021 roku, pozycja 2234 z późniejszymi zmianami) i § 3 Rozporządzeniem Prezesa Rady Ministrów z dnia 25 lipca 2016 roku w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (Dziennik Ustaw z 2016 roku pozycja 1101) zarządzam, co następuje:

Paragraf 1

1. W związku zarządzeniem Prezesa Rady Ministrów nr 233 z dnia 29 lipca 2022 roku w sprawie wprowadzenia stopnia alarmowego CRP, **został wprowadzony trzeci stopień alarmowy CHARLIE-CRP** (zagrożenia w cyberprzestrzeni) na całym terytorium Rzeczypospolitej Polskiej, obowiązujący od 1.08.2022 r. od godziny 00.00 do dnia 31.08.2022 r. do godziny 23.59.
2. Wobec powyższego zobowiązuję, w tym czasie, pracowników Referatu do spraw procesów IT, kierowników i pracowników komórek organizacyjnych oraz pracowników stanowisk samodzielnych Urzędu Miasta Ciechanów, kierowników wszystkich spółek miejskich i miejskich jednostek budżetowych do:
 - 1) wprowadzenia wzmożonego monitorowania stanu bezpieczeństwa systemów teleinformatycznych oraz:
 - a) monitorowania i weryfikowania, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej
 - b) sprawdzania dostępności usług elektronicznych,
 - c) dokonywania, w razie potrzeby, zmian w dostępie do systemów,
 - 2) informowania personel instytucji o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności personelu odpowiedzialnego za bezpieczeństwo systemów,
 - 3) sprawdzania kanałów łączności z innymi, właściwymi dla rodzaju stopnia alarmowego CRP, podmiotami biorącymi udział w reagowaniu kryzysowym,

- 4) dokonania weryfikacji ustanowionych punktów kontaktowych z zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego,
- 5) dokonania przeglądu stosownych procedur oraz zadań związanych z wprowadzeniem stopni alarmowych CRP, 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,
- 6) sprawdzenia aktualnego stanu bezpieczeństwa systemów i oceny wpływu zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń,
- 7) informowania na bieżąco o efektach przeprowadzanych działań zespoły reagowania na incydenty bezpieczeństwa teleinformatycznego.
- 8) zapewnienia dostępności w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów;
- 9) wprowadzenia całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania organizacji (jednostki) oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych;
- 10) wprowadzenia całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania organizacji (jednostki) oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów;
- 11) dokonania przeglądu dostępnych zasobów zapasowych pod względem możliwości ich wykorzystania w przypadku zaistnienia ataku;
- 12) przygotowania się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku, w tym:
 - a) dokonania przeglądu i ewentualnego audytu planów awaryjnych oraz systemów,
 - b) przygotowania się do ograniczenia operacji na serwerach, w celu możliwości ich szybkiego i bezawaryjnego zamknięcia.

Paragraf 2

1. O zaistniałych, niepokojących zdarzeniach i incydentach w działaniach systemów teleinformatycznych należy bezzwłocznie informować dyżurnego Miejskiego Centrum Zarządzania Kryzysowego (MCZK) Pana Radosława Lipowskiego – nr tel. 509 406 453. Pracownicy IT w poszczególnych jednostkach są zobowiązani do bezzwłocznego reagowania na zakłócenia pracy systemów.
2. Dyżurnego MCZK zobowiązuję do przekazywania otrzymywanych informacji i powiadomień do Powiatowego Centrum Zarządzania Kryzysowego w Ciechanowie lub Powiatowego Stanowiska Kierowania Państwowej Straży Pożarnej (w formie raportu doraźnego) oraz bieżącego informowania

Prezydenta Miasta Ciechanów o zaistniałych zakłóceniach pracy systemów teleinformatycznych.

Paragraf 3

Nadzór nad wdrożeniem i prawidłowym funkcjonowaniem zarządzenia powierza się Sekretarzowi Miasta.

Paragraf 4

Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta Ciechanów
Krzysztof Kosiński