INFORMACJA

Zgodnie z zarządzeniem Prezesa Rady Ministrów, na terytorium całego kraju **drugi stopień alarmowy CRP (CHARLIE–CRP) obowiązuje do 31 maja, do godz. 23.59**. Ostrzeżenie zostało wprowadzone w celu przeciwdziałania zagrożeniom w cyberprzestrzeni. Ponadto na terenie całego kraju wprowadzony został **drugi stopień alarmowy BRAVO**oraz **drugi stopień alarmowy BRAVO wobec polskiej infrastruktury energetycznej poza granicami kraju. Obowiązują one również do 31 maja, do godz. 23.59**.

Stopień alarmowy CRP wprowadził Prezes Rady Ministrów na podstawie przepisów ustawy o działaniach antyterrorystycznych. Stopień BRAVO jest drugim w czterostopniowej skali stopni alarmowych i można go wprowadzić w przypadku zaistnienia zwiększonego i przewidywalnego zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym, kiedy jednak konkretny cel ataku nie został zidentyfikowany.

Stopnie CRP wprowadza się w sytuacji zagrożenia o charakterze terrorystycznym, które dotyczy systemów teleinformatycznych administracji publicznej lub systemów, które wchodzą w skład infrastruktury krytycznej. ALFA to pierwszy stopień alarmu, BRAVO – drugi, CHARLIE – trzeci, a DELTA – czwarty, najwyższy.

Stopień alarmowy BRAVO zobowiązuje policję, straż graniczną oraz żandarmerię wojskową do noszenia broni długiej oraz kamizelek kuloodpornych. Ponadto należy przeprowadzać kontrole pojazdów, osób oraz budynków publicznych w rejonach zagrożonych oraz zapewnić personel na wypadek zdarzeń terrorystycznych.

Zadania organów państwa związane z wprowadzeniem stopni alarmowych CRP zostały określone w rozporządzeniu Prezesa Rady Ministrów z 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP. Do zadań tych należą m.in.:

* całodobowe dyżury administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa tych systemów
* przegląd zasobów pod względem możliwości ich wykorzystania w przypadku zaistnienia ataku
* przygotowanie się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku, w tym szybkiego i bezawaryjnego zamknięcia serwerów.

**Wszelkie niepokojące i nietypowe sytuacje oraz zagrożenia powinny być zgłaszane policji za pośrednictwem numeru telefonu 112.**