SPO – 42 CRP	Rodzaj dokumentu	Moduł zadaniowy	Data	30.06.2016r.
	Nazwa dokumentu	PRZEDSIĘWZIĘCIA REALIZOWANE W RAMACH II STOPNIA ALRMOWEGO CRP	Podmiot opracowujący	Wójt Gminy

I. Cel zadania

Określenie działań umożliwiających realizację zadań po wprowadzeniu stopni alarmowych CRP, w związku z wystąpieniem zagrożenia terrorystycznego lub sabotażu.

II. Warunki operacyjne realizacji zadania

Wójt / Sekretarz Gminy, Informatyk, pracownicy Urzędu Gminy, kierownicy jednostek organizacyjnych.

III. Przedsięwzięcia do wykonania w ramach zadania

Przedsięwzięcia	Podstawy (prawne) działań
Przeciwdziałanie wystąpienia zdarzeń o charakterze terrorystycznym lun sabotażowym i minimalizacji jego skutków. Realizacja zadań w ramach stopni alarmowych CRP dla zagrożeń w cyberprzestrzeni	➢ Art. 17, ust. 2 pkt 5 ustawy z dnia 26 kwietnia 2007r. **o zarządzaniu kryzysowym** (Dz. U. Nr 89, poz. 590, z późn. zm.); ➢ Zarządzenie Nr 18 Prezesa Rady Ministrów z dnia 02 marca 2016r. **w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego** ➢ Zarządzenie Nr 61 Wojewody Opolskiego z dnia 23 maja 2016r. **w sprawie określenia sposobu realizacji zadań po wprowadzeniu stopni alarmowych i stopni alarmowych dla zagrożeń w cyberprzestrzeni Rzeczypospolitej Polskiej na terenie województwa opolskiego**

IV. Koncepcja działania

A. Tryb uruchamiania zasobów	Wykonawcy
Wydanie zarządzenia w sprawie wprowadzenia I stopnia alarmowego CRP	➢ Wójt Gminy / Sekretarz Gminy
B. Organizacja kierowania / dowodzenia	**Wykonawcy**
Realizacja zadań określonych w zarządzeniach wprowadzających stopień alarmowy I CRP, oraz :	➢ Wójt Gminy / Sekretarz Gminy
C. Przedsięwzięcia reagowania	**Wykonawcy**
1. Zapewnić gotowość do niezwłocznego podejmowania działań przez administratorów systemów kluczowych dla funkcjonowania organizacji, a) administrator jest zobowiązany do podejmowania działań mających na celu zebezpieczenie sieci, systemów dziedzinowych oraz backupowych 2. Wprowadzić dyżury w trybie alarmowym osób uprawnionych do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych, a) dyżur w jednostce administratora systemów b) analiza sytuacji, ocena ryzyka dla sieci LAN 3. Wprowadzić wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych, w tym w szczególności wykorzystując zlecenia Szefa Agencji Bezpieczeństwa Wewnętrzengo lub komórek odpowiedzialnych za system reagowania, zgodnie z właściwością oraz : a) monitorować i weryfikować, czy nie doszło do naruszenia bezpieczeństwa, • weryfikacja logów z urządzeń brzegowych, • analiza pod kątem wykrywania ataków na sieć LAN • analiza ruchu mail pod kątem ataku • analiza logów ze switchy pod kątem nieautoryzownego wpięcia w sieć LAN b) sprawdzić dostępność usług elektronicznych, • sprawdzenie łącza internetowego • testowe łączenie na sieciowych urządzeniach zastępczych c) w razie potrzeby dokonywać zmian w dostępie do infrastruktury teleinformatycznej • awaryjna zmiana haseł do urządzeń brzegowych	➢ Wójt Gminy / Sekretarz Gminy / informatyk

• awaryjna zmiana haseł do systemów sieciowych • awaryjna zmiana haseł do systemów dziedzinowych • awaryjna zmiana haseł do systemów backupowych	
D. Wsparcie bieżące	**Wykonawcy**
Monitorowanie zadań realizowanych przez jednostki organizacyjne i pomocnicze Urzędu Gminy	➢ Wójt Gminy / Sekretarz Gminy / informatyk

V. Potrzeby w przypadku przedłużających się działań

W przypadku przedłużających się działań, należy zapewnić dostęp do żywności, jak również zapewnić środki higieny osobistej.

VI. Budżet zadania