Urząd Gminy Żurawica
ul. Ojca Św. Jana Pawła II 1
37-710 Żurawica

Załącznik nr 1 do zarządzenia nr 29/2023
Wójta Gminy Żurawica

Nr 7	*Rodzaj dokumentu*	*MODUŁ ZADANIOWY*	*Data*	*2023*
	Treść zadania	*Przedsięwzięcia realizowane w ramach III stopnia alarmowego CHARLIE - CRP*	*Wykonawca zadania*	*WÓJT GMINY ŻURAWICA*

Po wprowadzeniu trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP) należy wykonać zadania wymienione dla pierwszego i drugiego stopnia alarmowego CRP oraz kontynuować lub sprawdzić wykonanie tych zadań, jeśli wcześniej został wprowadzony stopień ALFA-CRP lub BRAVO-CRP. Ponadto należy wykonać w szczególności następujące zadania:

Organy administracji publicznej realizują zadania w ramach poszczególnych stopni alarmowych lub stopni alarmowych CRP w ramach opracowanych procedur modułów zadaniowych, dla każdego stopnia, zawierającymi w szczególności:

1) **wykaz odbiorców informacji i sposób ich informowania o wprowadzonym stopniu;**
2) **zadania do wykonania w każdym ze stopni;**
3) **zasady wprowadzania stopnia alarmowego lub stopnia alarmowego CRP przez ministra (kierownika urzędu centralnego, wojewodę).**

W przypadku wprowadzenia stopni alarmowych CRP, organy administracji publicznej mogą wykonać dodatkowe przedsięwzięcia

w zakresie:

1) **wdrożenia dodatkowych elementów ochrony, w celu wzmocnienia bezpieczeństwa obiektów, obszarów i urządzeń - zgodnie z art. 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia ,**
2) **wprowadzenia zakazu przeprowadzania imprez masowych - na podstawie art. 34 ust. 1 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych;**
3) **wprowadzenia zakazu organizacji zgromadzeń - na podstawie art. 14 ustawy z dnia 24 lipca 2015 r. - Prawo o zgromadzeniach;**
4) **wprowadzenia ograniczeń w przewozie towarów niebezpiecznych - na podstawie art. 60 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie ,**
5) **wprowadzenia zakazów lub ograniczeń w ruchu lotniczym - zgodnie z art. 119 ustawy z dnia 3 lipca 2002 r. - Prawo lotnicze ,**
6) **wprowadzenia zakazu noszenia broni - na podstawie art. 33 ustawy z dnia 21 maja 1999 r. o broni i amunicji ,**
7) **wprowadzenia ograniczeń w spożyciu żywności uznanej za niebezpieczną - na podstawie art. 27 ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej ,**
8) **wprowadzenia ograniczeń w obrocie niebezpiecznymi produktami leczniczymi lub wyrobami medycznymi - na podstawie art. 121 ustawy z dnia 6 września 2001 r. - Prawo farmaceutyczne ,**

9) wprowadzenia zakazów lub nakazów określonego zachowania się - na podstawie art. 48 ustawy z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej ,

10) zapobieżenia lub ograniczenia zagrożenia ochrony żeglugi i portów - na podstawie art. 26 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich ,

Po wprowadzeniu pierwszego stopnia alarmowego CRP (stopień ALFA-CRP) należy wykonać w szczególności następujące zadania:

1) wprowadzić wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, w szczególności wykorzystując zalecenia Szefa Agencji Bezpieczeństwa Wewnętrznego lub komórek odpowiedzialnych za systemy reagowania zgodnie z właściwością, oraz:
   a) monitorować i weryfikować, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej,
   b) sprawdzić dostępność usług elektronicznych,
   c) dokonać, w razie potrzeby, zmian w dostępie do systemów;
2) poinformować personel instytucji, w szczególności odpowiedzialny za bezpieczeństwo systemów teleinformatycznych, o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy;
3) zapewnić dostępność w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów teleinformatycznych;
4) sprawdzić kanały łączności z innymi podmiotami biorącymi udział w reagowaniu kryzysowym właściwymi dla rodzaju stopnia alarmowego CRP, zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla rodzaju działania organizacji oraz ministrem właściwym do spraw informatyzacji;
5) dokonać 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 do przywrócenia poprawności funkcjonowania systemu;
6) sprawdzić aktualny stan bezpieczeństwa infrastruktury teleinformatycznej i ocenić wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń;
7) informować na bieżąco o efektach przeprowadzanych działań zespoły reagowania na incydenty bezpieczeństwa teleinformatycznego właściwe dla rodzaju działania organizacji oraz współdziałające centra zarządzania kryzysowego, a także ministra właściwego do spraw informatyzacji.

Po wprowadzeniu drugiego stopnia alarmowego CRP (stopień BRAVO-CRP) należy wykonać zadania wymienione dla pierwszego stopnia alarmowego CRP oraz kontynuować lub sprawdzić wykonanie tych zadań, jeśli wcześniej został wprowadzony stopień ALFA-CRP. Ponadto należy wykonać w szczególności następujące zadania:

1) zapewnić gotowość do niezwłocznego podejmowania działań przez administratorów systemów kluczowych dla funkcjonowania organizacji;
2) wprowadzić całodobowe dyżury w trybie alarmowym osób uprawnionych do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych;
3) wprowadzić wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych, w tym 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 naruszenia bezpieczeństwa komunikacji elektronicznej,

b) **sprawdzać dostępność usług elektronicznych,**

c) **w razie potrzeby dokonywać zmian w dostępie do infrastruktury teleinformatycznej.**

1) **dokonać przeglądu dostępnych zasobów zapasowych pod względem możliwości ich wykorzystania w wypadku zaistnienia ataku;**

2) **przygotować się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku, w tym m.in.:**

a) **dokonać przeglądu i ewentualnego audytu planów awaryjnych oraz infrastruktury teleinformatycznej,**

b) **przygotować się do ograniczenia operacji na serwerach, w celu możliwości ich szybkiego i bezawaryjnego zamknięcia.**

Wójt Gminy Żurawica

Tomasz Szeleszczuk