Ministerstwo
Spraw Wewnętrznych
i Administracji

Paweł SZEFERNAKER
Sekretarz Stanu
Pełnomocnik Rządu
ds. Współpracy z Samorządem Terytorialnym
DAP-WAR—0748-12

Warszawa, dnia 22 lutego 2022 r.

Panie i Panowie
Marszałkowie Województw, Prezydenci
Miast, Starostowie, Burmistrzowie
i Wójtowie

Szanowni Państwo!

W związku z wprowadzeniem zarządzeniem nr 40 Prezesa Rady Ministrów z dnia 21 lutego 2022 r., trzeciego stopnia alarmowego CRP (stopnia CHARLIE-CRP) – obowiązującego od 21 lutego 2022 r., od godz. 21.00, do 4 marca 2022 r., do godz. 23.59 pozwalam sobie przekazać Państwu informację nt. sposobów postępowania i przedsięwzięć mających na celu przeciwdziałanie i minimalizację wpływu skutków ewentualnych ataków w cyberprzestrzeni na funkcjonowanie administracji publicznej.

W kontekście wprowadzonego na podstawie art. 16 ust. 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2021 r. poz. 2234), zarządzeniem nr 40 Prezesa Rady Ministrów z dnia 21 lutego 2022 r., trzeciego stopnia alarmowego CRP (stopnia CHARLIE-CRP) – obowiązującego od 21 lutego 2022 r., od godz. 21.00, do 4 marca 2022 r., do godz. 23.59 – należy podkreślić, że zgodnie z art. 16 ust. 4 ww. ustawy, **wprowadzenie stopnia alarmowego lub stopnia alarmowego CRP stanowi podstawę do realizacji przez organy administracji publicznej oraz kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego przedsięwzięć:**

- określonych w **rozporządzeniu Prezesa Rady Ministrów z dnia 25 lipca 2016 r. *w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP***, wynikających z ich kompetencji ustawowych;
- przedsięwzięć i procedur zarządzania kryzysowego, jeżeli zostały przewidziane dla danego stopnia alarmowego lub stopnia alarmowego CRP w związku z wystąpieniem zdarzenia o charakterze terrorystycznym i nie zostały uwzględnione ww. rozporządzeniu.

Organy administracji publicznej oraz kierownicy służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego wykonują przedsięwzięcia, w ramach poszczególnych stopni alarmowych i stopni alarmowych CRP, **we współpracy z właścicielami, posiadaczami samoistnymi i posiadaczami zależnymi obiektów infrastruktury krytycznej, w zakresie ochrony tych obiektów. To właśnie w tym aspekcie przede wszystkim należy**

upatrywać roli jednostek samorządu terytorialnego w kontekście wprowadzonego stopnia alarmowego CRP.

Z kolei **właściciele, posiadacze samoistni i posiadacze zależni obiektów infrastruktury krytycznej uwzględniają, na potrzeby współpracy szczegółowy zakres przedsięwzięć określonych w ww. rozporządzeniu** *w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP.*

W przypadku stopnia CHARLIE-CRP, poza zadaniami przewidzianymi w rozporządzeniu dla niższych stopni alarmowych CRP, tj.:

- wprowadzeniem wzmożonego monitorowania stanu bezpieczeństwa systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, w tym: monitorowaniem i weryfikowaniem, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej, sprawdzaniem dostępność usług elektronicznych oraz dokonywaniem, w razie potrzeby, zmian w dostępie do systemów;
- poinformowaniem personelu instytucji o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności personelu odpowiedzialnego za bezpieczeństwo systemów teleinformatycznych;
- sprawdzeniem kanałów łączności z innymi, właściwymi podmiotami biorącymi udział w reagowaniu kryzysowym, dokonaniem weryfikacji ustanowionych punktów kontaktowych z zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla rodzaju działania organizacji oraz ministrem właściwym do spraw informatyzacji;
- dokonaniem przeglądu stosownych procedur oraz zadań związanych z wprowadzeniem stopni alarmowych CRP, w szczególności dokonaniem 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;
- sprawdzeniem aktualnego stanu bezpieczeństwa systemów i oceną wpływu zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń;
- informowaniem na bieżąco o efektach przeprowadzanych działań zespołów reagowania na incydenty bezpieczeństwa teleinformatycznego właściwych dla rodzaju działania organizacji oraz współdziałających centrów zarządzania kryzysowego, a także ministra właściwego do spraw informatyzacji;
- zapewnieniem dostępności w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów;
- wprowadzeniem całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych.

należy również:

- dokonać przeglądu dostępnych zasobów zapasowych pod względem możliwości ich wykorzystania w przypadku zaistnienia ataku;
- przygotować się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku, w tym:
    - dokonać przeglądu i ewentualnego audytu planów awaryjnych oraz systemów,
    - przygotować się do ograniczenia operacji na serwerach, w celu możliwości ich szybkiego i bezawaryjnego zamknięcia.

Istotnym jest, że zarówno informacja o wprowadzeniu stopnia alarmowego do właściwych podmiotów, jak i informacje o realizacji przedsięwzięć związanych z wprowadzeniem stopnia alarmowego powinny być przekazywane bezpośrednio z i do **Rządowego Centrum Bezpieczeństwa**. Po otrzymaniu informacji o wprowadzeniu stopnia alarmowego lub stopnia alarmowego CRP, organy administracji publicznej oraz kierownicy służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego niezwłocznie potwierdzają Rządowemu Centrum Bezpieczeństwa fakt otrzymania informacji o wprowadzeniu stopnia alarmowego lub stopnia alarmowego CRP oraz przekazują raport o stanie realizacji zadań wynikających z wprowadzonego stopnia, w czasie nie dłuższym niż 12 godzin od otrzymania informacji.

Ponadto, zgodnie z ustawą o działaniach antyterrorystycznych (art. 4), organy administracji publicznej, właściciele i posiadacze obiektów, instalacji, urządzeń infrastruktury administracji publicznej lub infrastruktury krytycznej współpracują z organami, służbami i instytucjami właściwymi w sprawach bezpieczeństwa i zarządzania kryzysowego oraz przekazują niezwłocznie **Szefowi Agencji Bezpieczeństwa Wewnętrznego** będące w ich posiadaniu informacje dotyczące zagrożeń o charakterze terrorystycznym dla infrastruktury administracji publicznej lub infrastruktury krytycznej, w tym zagrożeń dla funkcjonowania systemów i sieci energetycznych, wodno-kanalizacyjnych, ciepłowniczych oraz teleinformatycznych istotnych z punktu widzenia bezpieczeństwa państwa.

W przypadku powzięcia informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym zagrażającego infrastrukturze administracji publicznej lub infrastrukturze krytycznej, życiu lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku, **Szef ABW może wydawać polecenia organom i podmiotom, zagrożonym tymi zdarzeniami, mające na celu przeciwdziałanie zagrożeniom, ich usunięcie albo minimalizację, oraz przekazywać im informacje niezbędne do tego celu.** Organy i podmioty informują natomiast Szefa ABW o podjętych działaniach w tym zakresie.

Informując o powyższym – jednocześnie przypominam, że organem właściwym w sprawach zarządzania kryzysowego na obszarze województwa jest wojewoda. Organem pomocniczym wojewody jest wojewódzki zespół zarządzania kryzysowego.

Proszę Państwa o ścisłą współpracę z wojewodami, którzy koordynują działania związane z obecną sytuacją kryzysową na terenie województw.

Z wyrazami szacunku

Paweł [illegible]

ul. Stefana Batorego 5
02-591 Warszawa, Polska
mswia.gov.pl
tel. +48 22 60 147 41