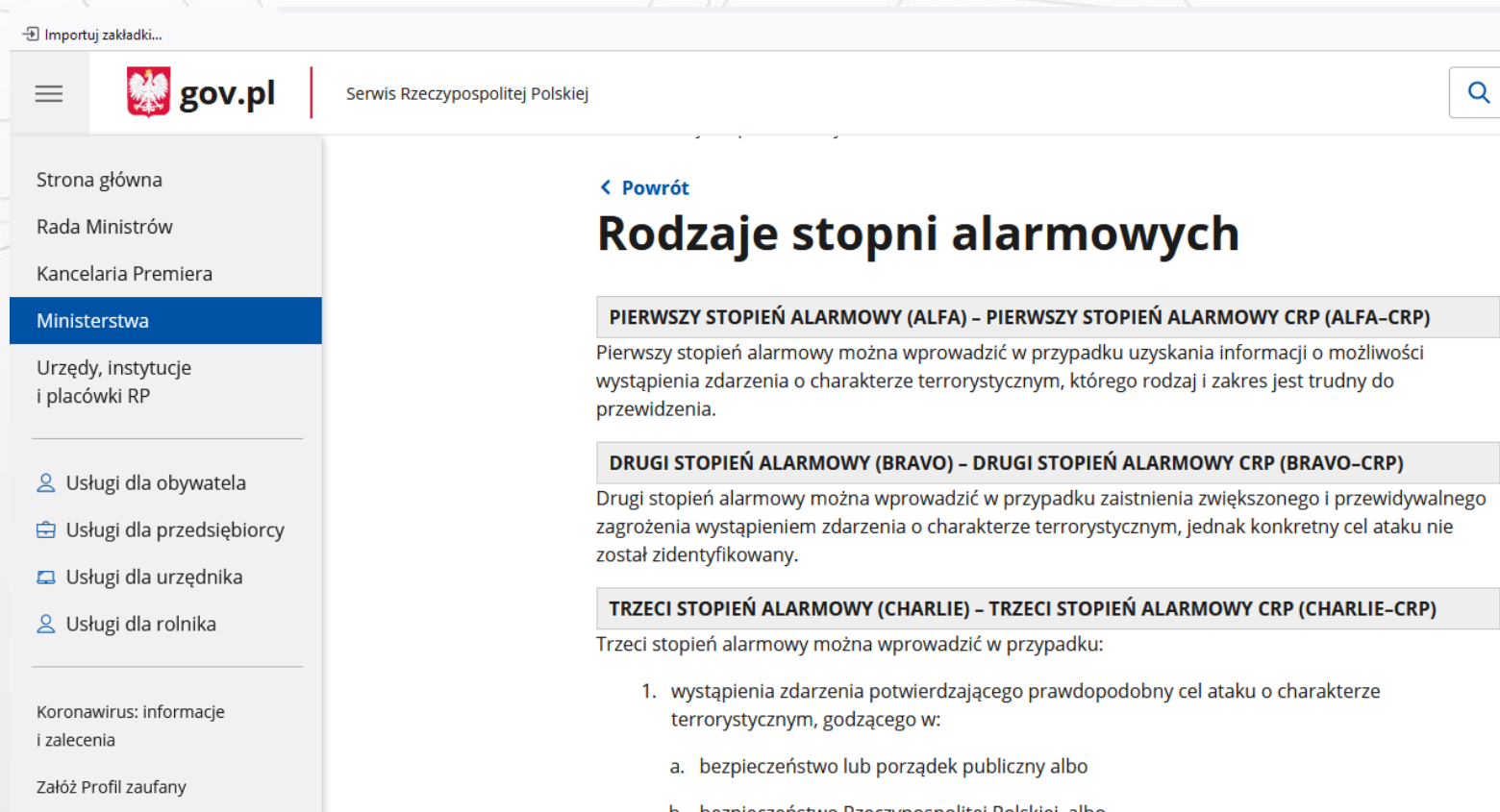


Stopnie alarmowe – podstawowe informacje



Importuj zakładki...

gov.pl | Serwis Rzeczypospolitej Polskiej

- Strona główna
- Rada Ministrów
- Kancelaria Premiera
- Ministerstwa**
- Urzędy, instytucje i placówki RP

- Usługi dla obywatela
- Usługi dla przedsiębiorcy
- Usługi dla urzędnika
- Usługi dla rolnika

Koronawirus: informacje i zalecenia

Załącz Profil zaufany

[< Powrót](#)

Rodzaje stopni alarmowych

PIERWSZY STOPIEŃ ALARMOWY (ALFA) – PIERWSZY STOPIEŃ ALARMOWY CRP (ALFA-CRP)

Pierwszy stopień alarmowy można wprowadzić w przypadku uzyskania informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym, którego rodzaj i zakres jest trudny do przewidzenia.

DRUGI STOPIEŃ ALARMOWY (BRAVO) – DRUGI STOPIEŃ ALARMOWY CRP (BRAVO-CRP)

Drugi stopień alarmowy można wprowadzić w przypadku zaistnienia zwiększonego i przewidywalnego zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym, jednak konkretny cel ataku nie został zidentyfikowany.

TRZECI STOPIEŃ ALARMOWY (CHARLIE) – TRZECI STOPIEŃ ALARMOWY CRP (CHARLIE-CRP)

Trzeci stopień alarmowy można wprowadzić w przypadku:

- wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym, godzącego w:
 - bezpieczeństwo lub porządek publiczny albo
 - bezpieczeństwo Rzeczypospolitej Polskiej albo

<https://www.gov.pl/web/mswia/rodzaje-stopni-alarmowych>

Pierwszy stopień alarmowy – stopień ALFA -CRP

- wprowadzić wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, zwanych dalej „systemami”
- monitorować i weryfikować, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej,
- sprawdzać dostępność usług elektronicznych,
- dokonywać, w razie potrzeby, zmian w dostępie do systemów;
- poinformować personel instytucji o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności personel odpowiedzialny za bezpieczeństwo systemów;
- sprawdzić kanały łączności z innymi, właściwymi dla rodzaju stopnia alarmowego CRP, podmiotami biorącymi udział w reagowaniu kryzysowym, dokonać weryfikacji ustanowionych punktów kontaktowych z zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla rodzaju działania organizacji oraz ministrem właściwym do spraw informatyzacji;

Pierwszy stopień alarmowy – stopień ALFA -CRP cd.

- 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 na przywrócenie poprawności funkcjonowania systemu;
- sprawdzić aktualny stan bezpieczeństwa systemów i ocenić wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń;
- 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.

Drugi stopień alarmowy – stopień BRAVO -CRP

- 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, jeżeli wcześniej był wprowadzony stopień ALFA-CRP.

Ponadto należy:

- zapewnić dostępność w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów;
- wprowadzić całodobowe dyżury administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych.

Trzeci stopień alarmowy – stopień CHARLI-CRP

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, jeżeli wcześniej był wprowadzony stopień ALFA-CRP lub BRAVO-CRP.

Ponadto należy wykonać w szczególności następujące zadania:

- wprowadzić całodobowe dyżury administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów;
- 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.

Czwarty stopień alarmowy – stopień DELTA-CRP

Po wprowadzeniu czwartego stopnia alarmowego CRP (stopień DELTA-CRP) należy wykonać zadania wymienione dla pierwszego, drugiego i trzeciego stopnia alarmowego CRP oraz kontynuować lub sprawdzić wykonanie tych zadań, jeżeli wcześniej był wprowadzony stopień ALFA-CRP, BRAVO-CRP lub CHARLIE CRP.

Ponadto należy wykonać w szczególności następujące zadania:

- uruchomić plany awaryjne lub plany ciągłości działania organizacji w sytuacjach awarii lub utraty ciągłości działania;
- stosownie do sytuacji przystąpić do realizacji procedur przywracania ciągłości działania.

Stopnie alarmowe w praktyce Urzędu Miasta

Pierwszy stopień alarmowy – stopień ALFA-CRP

ZADANIA DOTYCZĄ WSZYSTKICH PRACOWNIKÓW.

- zachowania zwiększonej **czujności** (e-maile, smsy, telefony)
- zabezpieczenie **kontaktów** telefonicznych z pracownikami (kanał łączności)
- sprawdzenie stosowanych **procedur** (zabezpieczenie danych, logowanie)
- sprawdzenie stanu **bezpieczeństwa** (aktualność windows, przeglądarka, NOD32ESET)
- **administratorzy na bieżąco informują o stanie przygotowania i incydentach (WZK)**
- **zgłaszanie i reagowanie na incydenty** (stosowne instytucje)
- przekazywać informacje o zagrożeniach i zdarzeniach do inspektora ochrony danych lub osoby wyznaczonej do kontaktu z NASK i instytucjami odpowiedzialnymi za bezpieczeństwo teleinformatyczne.

Drugi stopień alarmowy – stopień BRAVO–CRP

Dodatkowe obowiązki:

- dostępność administratorów systemów serwerowych (KSAT, INTRADOK, VULCAN, TKM, TURBOEWID, EWID, ZSIP, TECHNIKA, CEPIK, POCZTA)
- całodobowe dyżury administratorów bezpieczeństwa sieci i zasobów serwerowych
- Informowanie, raportowanie

Trzeci stopień alarmowy – stopień CHARLIE-CRP

Dodatkowe obowiązki

- całodobowe dyżury personelu uprawnionego do podejmowania decyzji
- przegląd kopii zapasowych
- Informowanie, raportowanie

Czwarty stopień alarmowy – stopień DELTA-CRP

Dodatkowe obowiązki:

- Plan awaryjny i ciągłości działania ,
- Dodatkowe zabezpieczanie kopii danych
- Przewidywana praca bez dostępu do internetu (utrzymanie działania systemów serwerowych)
- Możliwość wygaszenia części systemów serwerowych.
- Zabezpieczenie zasilania awaryjnego
- Utrzymanie dostępu do danych krytycznych
- Realizacja procedur odtworzeniowych środowisk i systemów teleinformatycznych
- Zasilanie odtworzonych systemów danych z kopii
- Informowanie, raportowanie

ZADAJMY SOBIE PYTANIE JAK WYDZIAŁ MA FUNKCJONOWAĆ BEZ SYSTEMÓW

ZADAJMY SOBIE PYTANIE JAK WYDZIAŁ/REFERAT/ZESPÓŁ MOŻE FUNKCJONOWAĆ BEZ SYSTEMÓW ?

Janusz Różycki - Inspektor Ochrony Danych Urzędu Miasta Tarnowa,

iod@umt.tarnow.pl