Ochrona przed atakami DDoS

1. Wzmożenie czujności w zakresie dostępności systemów i usług w sieci Internet.
2. Przygotowanie się do ograniczenia ruchu do obszaru RP w przypadku eskalacji zagrożenia.
3. Sprawdzenie zdolności zapewnienia ciągłości działania usług elektronicznych, systemów oraz sieci teleinformatycznych w przypadku wystąpienia ataków DDoS.
4. Sprawdzenie zdolności zapewnienia środków mitygacyjnych w postaci rozwiązań ochrony przed atakami typu DDoS.
5. Sprawdzenie zdolności Państwa dostawców telekomunikacyjnych do identyfikacji oraz izolacji ruchu DDoS, w tym czasu potrzebnego na przywrócenia dostępności infrastruktury dla Państwa usługi.
6. W przypadku ataku należy być gotowym na uruchomienie statycznej strony w celu zapewnienia dostępności podstawowych informacji.
7. Stosowanie procedury uwzględniającej utrzymywanie stałego kanału komunikacji z dostawcą telekomunikacyjnym, czy też dostawcą usług elektronicznych w celu niezwłocznego podejmowania działań obrony przed atakami typu DDoS, w szczególności informowania na bieżąco o dostępności łącza, usługi jak również zdolności do wprowadzenia izolacji ruchu.