Poz. 208

Narodowe Centrum Kryptologii

DECYZJA Nr 275/MON
MINISTRA OBRONY NARODOWEJ

z dnia 13 lipca 2015 r.

w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej

Na podstawie art. 2 pkt 6a ustawy z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz. U. z 2013 r. poz. 189 i 852 oraz z 2014 r. poz. 932) oraz § 1 pkt 1 lit. a i d, pkt 2 lit. e i § 2 pkt 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426 oraz z 2014 r. poz. 933), w związku z § 5 ust. 2 pkt 3 regulaminu organizacyjnego Ministerstwa Obrony Narodowej, stanowiącego załącznik do zarządzenia Nr 40/MON Ministra Obrony Narodowej z dnia 22 listopada 2006 r. w sprawie regulaminu organizacyjnego Ministerstwa Obrony Narodowej (Dz. Urz. Min. Obr. Nar. Nr 21, poz. 270, z późn. zm.[1)]) ustala się, co następuje:

1. Użyte w decyzji określenia oznaczają:
   1) administrator systemu teleinformatycznego - osobę lub zespół osób, niepełniących funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych w danej jednostce organizacyjnej za funkcjonowanie jawnego lub niejawnego systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego;
   2) cyberprzestrzeń - cyberprzestrzeń w rozumieniu art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2014 r. poz. 1815 oraz z 2015 r. poz. 529);

[1)] Zmiany wymienionego zarządzenia zostały ogłoszone w Dz. Urz. Min. Obr. Nar. z 2007 r. Nr 4, poz. 38, Nr 6, poz. 73, Nr 17, poz. 176 i Nr 21, poz. 209, z 2008 r. Nr 8, poz. 85, Nr 15, poz. 188, Nr 20, poz. 260 i Nr 23, poz. 287, z 2009 r. Nr 2, poz. 17, z 2010 r. Nr 10, poz. 106 i Nr 23, poz. 304, z 2011 r. Nr 5, poz. 54, z 2012 r. poz. 106, 307, 313 i 363, z 2013 r. poz. 157, 231 i 356, z 2014 r. poz. 88 oraz z 2015 r. poz. 31 i 68.

3) dokumentacja bezpieczeństwa teleinformatycznego - dokumentację w rozumieniu § 25 i 26 rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 159, poz. 948);
4) incydent bezpieczeństwa teleinformatycznego - pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji, które wiążą się lub mogą wiązać się z utratą ich poufności, dostępności lub integralności;
5) incydent komputerowy - pojedyncze zdarzenie lub seria zdarzeń dotyczących sprzętu komputerowego lub jego oprogramowania, stanowiących część incydentu bezpieczeństwa teleinformatycznego;
6) inspektor bezpieczeństwa teleinformatycznego – pracownika pionu ochrony odpowiedzialnego za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji;
7) jednostka organizacyjna - Ministerstwo Obrony Narodowej oraz jednostkę organizacyjną podległą Ministrowi Obrony Narodowej lub przez niego nadzorowaną;
8) komórka organizacyjna - komórkę organizacyjną Ministerstwa Obrony Narodowej w rozumieniu § 2 pkt 5 regulaminu organizacyjnego Ministerstwa Obrony Narodowej, stanowiącego załącznik do zarządzenia Nr 40/MON Ministra Obrony Narodowej z dnia 22 listopada 2006 r. w sprawie regulaminu organizacyjnego Ministerstwa Obrony Narodowej;
9) kierownik jednostki (komórki) organizacyjnej - dowódcę, szefa, dyrektora, komendanta lub inną osobę kierującą działalnością jednostki lub komórki organizacyjnej, w tym osobę czasowo pełniącą obowiązki;
10) organizator systemu teleinformatycznego - kierownika jednostki organizacyjnej organizującej system teleinformatyczny lub upoważnionego przez niego kierownika komórki organizacyjnej;
11) pełnomocnik ochrony - pełnomocnika kierownika jednostki organizacyjnej do spraw ochrony informacji niejawnych;
12) reagowanie - zachowanie lub postępowanie, jako odpowiedź na zaistniałe zdarzenie;
13) SRnIK - System Reagowania na Incydenty Komputerowe resortu obrony narodowej (w kontaktach międzynarodowych określany jako MIL-CERT PL), zorganizowany w trzypoziomową strukturę, w skład której wchodzą:
    a) Centrum Koordynacyjne SRnIK, którego funkcję pełni właściwa komórka wewnętrzna Służby Kontrwywiadu Wojskowego,
    b) Centrum Wsparcia SRnIK, którego funkcję pełni właściwa komórka wewnętrzna Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych,
    c) administratorzy systemów teleinformatycznych w jednostkach i komórkach organizacyjnych;
14) system teleinformatyczny - system teleinformatyczny w rozumieniu art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2013 r. poz. 235 oraz z 2014 r. poz. 183);
15) środki do rejestracji i analizy zdarzeń - rozwiązania techniczne umożliwiające prowadzenie w czasie rzeczywistym w monitorowanym systemie teleinformatycznym rejestracji lub analizy określonych zdarzeń lub stanów;
16) zagrożenie - potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego;
17) zdarzenie - zmiana stanu systemu lub usługi, która wskazuje na możliwe naruszenie polityki bezpieczeństwa lub procedur zawartych w dokumentacji

bezpieczeństwa teleinformatycznego, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.

2. SRnIK organizuje się w celu zapewnienia koordynacji i realizacji procesów zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach teleinformatycznych oraz autonomicznych stanowiskach komputerowych organizowanych przez jednostki organizacyjne, z wyłączeniem systemów Żandarmerii Wojskowej wykorzystywanych bezpośrednio do prowadzenia działalności dochodzeniowo-śledczej oraz operacyjno-rozpoznawczej.
3. Nadzór nad funkcjonowaniem SRnIK w odniesieniu do systemów teleinformatycznych przeznaczonych do przetwarzania informacji jawnych sprawuje Pełnomocnik Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni.
4. Nadzór nad funkcjonowaniem SRnIK w odniesieniu do systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych sprawuje Szef Służby Kontrwywiadu Wojskowego.
5. Centrum Koordynacyjne SRnIK:
   1) określa ogólne zasady funkcjonowania SRnIK;
   2) współpracuje w zakresie ustalania formalno-prawnych zasad funkcjonowania SRnIK oraz planów jego rozwoju w wymiarze krajowym i międzynarodowym z:
      a) Agencją Bezpieczeństwa Wewnętrznego,
      b) Żandarmerią Wojskową,
      c) Departamentem Ochrony Informacji Niejawnych Ministerstwa Obrony Narodowej,
      d) Organizatorem Systemu Funkcjonalnego Wsparcia Dowodzenia,
      e) Centrum Wsparcia SRnIK w zakresie ustalania ogólnych zasad funkcjonowania SRnIK,
      f) Centrum Koordynacyjnym systemu reagowania na incydenty komputerowe Organizacji Traktatu Północnoatlantyckiego,
      g) krajowymi i międzynarodowymi organami koordynującymi systemy reagowania na incydenty komputerowe,
      h) pionami ochrony informacji niejawnych organizatorów systemów niejawnych;
   3) koordynuje realizację procedur obsługi incydentów bezpieczeństwa teleinformatycznego oraz współuczestniczy w monitorowaniu stanu bezpieczeństwa resortowych systemów teleinformatycznych, w których wdrożono techniczne środki do rejestracji i analizy zdarzeń;
   4) realizuje zadania wynikające z Planu Zarządzania Kryzysowego MON, Wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego oraz Planu Operacyjnego Funkcjonowania Działu Administracji Rządowej Obrona Narodowa w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny;
   5) wspólnie z Centrum Wsparcia SRnIK dokonuje cyklicznych analiz poziomu bezpieczeństwa resortowych systemów teleinformatycznych poprzez analizę ilości, a także istotności wykrywanych incydentów komputerowych oraz incydentów bezpieczeństwa teleinformatycznego – wyniki powyższych analiz przedstawiane są przynajmniej raz w roku odpowiednio: Pełnomocnikowi Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni oraz Szefowi Służby Kontrwywiadu Wojskowego;
   6) wspólnie z Centrum Wsparcia SRnIK oraz we współpracy z organizatorami systemów teleinformatycznych przeznaczonych do przetwarzania informacji jawnych, opracowuje projekty zaleceń i wytycznych z zakresu zapobiegania wystąpieniu w nich incydentów komputerowych oraz przedstawia je do

zatwierdzenia Pełnomocnikowi Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni;

7) w oparciu o informacje przekazywane przez Centrum Wsparcia SRnIK, opracowuje projekty zaleceń i wytycznych z zakresu zapobiegania wystąpieniu incydentów komputerowych w systemach teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych oraz przedstawia je do zatwierdzenia Szefowi Służby Kontrwywiadu Wojskowego;
8) bierze udział w pracach grup roboczych w ramach Organizacji Traktatu Północnoatlantyckiego oraz Unii Europejskiej, a także, w uzgodnieniu z Pełnomocnikiem Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni, reprezentuje resort obrony narodowej w kontaktach z organizacjami spoza resortu obrony narodowej, w zakresie reagowania na incydenty komputerowe w systemach teleinformatycznych;
9) prowadzi ewidencję systemów teleinformatycznych objętych SRnIK, na podstawie danych otrzymanych od organizatorów systemów teleinformatycznych;
10) reprezentuje SRnIK w zakresie koordynacji na szczeblu międzyresortowym i w stosunkach międzynarodowych.

6. Centrum Wsparcia SRnIK:
   1) na bieżąco współpracuje z Centrum Koordynacyjnym SRnIK;
   2) odpowiada za opracowanie i stałą aktualizację:
      a) „Podręcznika reagowania na incydenty komputerowe w resorcie obrony narodowej”,
      b) „Standardowych Procedur Operacyjnych SRnIK w resorcie obrony narodowej”,
      c) „Wytycznych do opracowania Lokalnych Procedur Operacyjnych SRnIK w jednostce organizacyjnej”;
   3) monitoruje stan bezpieczeństwa resortowych systemów teleinformatycznych, w których wdrożono techniczne środki do rejestracji i analizy zdarzeń;
   4) zbiera i analizuje informacje o zdarzeniach oraz tworzy na ich bazie okresowe raporty o stanie bezpieczeństwa w systemach teleinformatycznych dla potrzeb organizatorów systemów teleinformatycznych, Centrum Koordynacyjnego SRnIK oraz Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni;
   5) realizuje zadania w zakresie wsparcia technicznego dla bezpośredniej obsługi incydentów komputerowych przez administratorów systemów teleinformatycznych oraz współuczestniczy w obsłudze incydentów bezpieczeństwa teleinformatycznego w systemach teleinformatycznych według procedur, o których mowa w ppkt 2 lit. b, a w przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych, z uwzględnieniem postanowień zawartych w zatwierdzonej dokumentacji bezpieczeństwa teleinformatycznego;
   6) w przypadku wykrycia incydentu komputerowego lub incydentu bezpieczeństwa teleinformatycznego:
      a) może wnioskować do organizatora systemu teleinformatycznego w sprawie czasowego wyłączania, ograniczenia funkcjonalności lub zaniechania przetwarzania informacji w systemie lub części systemu teleinformatycznego przetwarzającego informacje niejawne, w którym stwierdzono wystąpienie takiego incydentu,
      b) za wiedzą organizatora systemu teleinformatycznego podejmuje decyzje o czasowym odłączeniu elementu systemu teleinformatycznego, w którym stwierdzono wystąpienie takiego incydentu, jeśli możliwe jest naruszenie poufności, integralności lub dostępności informacji

przetwarzanych w systemie teleinformatycznym posiadającym połączenie z siecią Internet lub jeśli przedmiotowy incydent może mieć negatywny wpływ na integralność lub dostępność tego systemu;

7) na bieżąco informuje organizatora systemu teleinformatycznego oraz Centrum Koordynacyjne SRnIK o zdarzeniach, incydentach komputerowych, zagrożeniach związanych z monitorowanym systemem teleinformatycznym oraz o wydanych w tym zakresie zaleceniach i wytycznych;
8) w zakresie reagowania na incydenty komputerowe i incydenty bezpieczeństwa teleinformatycznego współpracuje z:
   a) Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL,
   b) właściwymi pionami ochrony informacji niejawnych,
   c) Żandarmerią Wojskową i innymi organami uprawnionymi do ścigania przestępstw komputerowych - w zakresie bezpieczeństwa systemów teleinformatycznych w resorcie obrony narodowej oraz reagowania na podejrzenie popełnienia przestępstwa przeciwko ochronie informacji,
   d) Rządowym Centrum Bezpieczeństwa,
   e) Dowództwem Operacyjnym Rodzajów Sił Zbrojnych,
   f) Centrum Wsparcia systemu reagowania na incydenty komputerowe Organizacji Traktatu Północnoatlantyckiego,
   g) krajowymi i międzynarodowymi zespołami systemu reagowania na incydenty komputerowe,
   h) organizatorami systemów teleinformatycznych,
   i) kierownikami jednostek organizacyjnych i komórek organizacyjnych za pośrednictwem administratorów systemów teleinformatycznych;
9) dla personelu komórek i jednostek organizacyjnych organizuje:
   a) szkolenia z zakresów reagowania na incydenty komputerowe oraz incydenty bezpieczeństwa teleinformatycznego,
   b) praktyczne ćwiczenia reagowania na incydenty bezpieczeństwa teleinformatycznego w oparciu o platformę szkoleniową, w której odwzorowane jest funkcjonowanie rzeczywistych systemów teleinformatycznych;
10) prowadzi działania polegające na wydawaniu biuletynów informacyjnych, analizie infrastruktury teleinformatycznej oraz uczestniczy w opracowywaniu zaleceń i wytycznych zapobiegających wystąpieniu incydentów komputerowych;
11) we współdziałaniu z organizatorem systemu teleinformatycznego oraz z Centrum Koordynacyjnym SRnIK implementuje i stosuje środki techniczne i organizacyjne oraz narzędzia do zdalnego zarządzania i kontroli konfiguracji systemów teleinformatycznych, służące do zapobiegania, wykrywania i usuwania skutków incydentów komputerowych. W przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych, zastosowanie wyżej wymienionych rozwiązań uwzględnia się w szacowaniu ryzyka oraz dokumentacji bezpieczeństwa systemu teleinformatycznego. W powyższym zakresie organizator systemu teleinformatycznego uzgadnia dokumentację bezpieczeństwa z Centrum Wsparcia SRnIK;
12) na polecenie Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni lub Centrum Koordynacyjnego SRnIK lub wniosek organizatora systemu teleinformatycznego lub organu akredytującego, realizuje – w porozumieniu z organizatorem systemu teleinformatycznego, a w przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych, również z właściwym pionem ochrony i organem akredytującym – testy bezpieczeństwa i testy podatnościowe, mające na celu weryfikację poprawności funkcjonowania zabezpieczeń, ustalenie ich aktualnego stanu oraz rekomendowanie skutecznych rozwiązań;

13) na potrzeby obsługi incydentów bezpieczeństwa i prowadzonych działań informacyjnych prowadzi współdzielone z Centrum Koordynacyjnym SRnIK oraz Pełnomocnikiem do spraw Bezpieczeństwa Cyberprzestrzeni portale informacyjne;
14) udziela niezbędnej pomocy pełnomocnikom do spraw ochrony informacji niejawnych w przypadku prowadzenia przez nich postępowania wyjaśniającego wystąpienie incydentu komputerowego;
15) udziela niezbędnej pomocy administratorom systemów teleinformatycznych w trakcie obsługi incydentu komputerowego oraz przywracania funkcjonowania systemu teleinformatycznego po zaistniałym incydencie;
16) utrzymuje laboratorium techniczne na potrzeby analizy informatycznych nośników danych, kodów złośliwych oraz prowadzenia testów bezpieczeństwa i podatności;
17) w uzgodnieniu z Centrum Koordynacyjnym SRnIK, uczestniczy w pracach grup roboczych w zakresie reagowania na incydenty komputerowe w systemach teleinformatycznych przeznaczonych do przetwarzania informacji jawnych lub narodowych informacji niejawnych;
18) dokumenty, o których mowa w pkt 6 ppkt 2, przed zatwierdzeniem przez Organizatora Systemu Teleinformatycznego, podlegają uzgodnieniu z pełnomocnikiem do spraw ochrony informacji niejawnych Organizatora Systemu Teleinformatycznego.

7. Administratorzy systemów teleinformatycznych w komórkach i jednostkach organizacyjnych są zobowiązani do:
   1) realizacji procedur SRnIK w zakresie bezpośredniej, technicznej obsługi incydentów komputerowych oraz wykonywania doraźnych zaleceń Centrum Wsparcia SRnIK w zakresie przeciwdziałania naruszeniom polityk bezpieczeństwa oraz obsługi incydentów komputerowych i incydentów bezpieczeństwa teleinformatycznego;
   2) wdrożenia, w uzgodnieniu z kierownikiem jednostki organizacyjnej, „Lokalnych Procedur Operacyjnych SRnIK w jednostce organizacyjnej", w tym ujętych w dokumentacji bezpieczeństwa;
   3) nadzorowania użytkowników administrowanych przez nich jawnych systemów teleinformatycznych w zakresie przestrzegania ustalonych procedur bezpieczeństwa;
   4) współpracy, zgodnie z procedurami SRnIK, z Centrum Koordynacyjnym SRnIK oraz instytucjami określonymi w pkt 6 ppkt 8 lit. b i c w zakresie zabezpieczenia śladów i ustalenia przyczyn wystąpienia incydentu komputerowego oraz incydentu bezpieczeństwa teleinformatycznego;
   5) zgłaszania do Centrum Wsparcia SRnIK, a w przypadku systemów teleinformatycznych przetwarzających informacje niejawne, dodatkowo do inspektora bezpieczeństwa teleinformatycznego, wykrytych incydentów komputerowych oraz wszelkich zdarzeń mogących wpłynąć na naruszenie polityki bezpieczeństwa w administrowanych przez nich systemach teleinformatycznych;
   6) przesyłania niezwłocznie do Centrum Wsparcia SRnIK wskazanych przez niego próbek kodu lub materiałów umożliwiających prowadzenia analiz technicznych, zgodnie z procedurami SRnIK - w przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych, czynności te realizowane są na zasadach opisanych w dokumentacji bezpieczeństwa teleinformatycznego;
   7) informowania Centrum Wsparcia SRnIK, za pośrednictwem kierownika jednostki organizacyjnej, o zmianach personalnych i teleadresowych

administratorów funkcjonujących w jednostce organizacyjnej systemów teleinformatycznych.

8. Dokumenty, o których mowa w pkt 6 ppkt 2, szczegółowo regulujące zasady funkcjonowania SRnIK, przed zatwierdzeniem przez Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni, podlegają uzgodnieniu z:
   1) Centrum Koordynacyjnym SRnIK;
   2) Departamentem Ochrony Informacji Niejawnych;
   3) Żandarmerią Wojskową;
   4) organizatorem systemu teleinformatycznego, w części dotyczącej jego systemu;
   5) Organizatorem Systemu Funkcjonalnego Wsparcia Dowodzenia;
   6) Departamentem Strategii i Planowania Obronnego, w zakresie zachowania spójności dokumentów z Planem Zarządzania Kryzysowego MON, Wykazem przedsięwzięć i procedur systemu zarządzania kryzysowego oraz Planem Operacyjnym Funkcjonowania Działu Administracji Rządowej Obrona Narodowa w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny.
9. Kierownicy komórek i jednostek organizacyjnych zapewnią:
   1) możliwość realizacji zadań przez pełnomocników ochrony, inspektorów bezpieczeństwa teleinformatycznego i administratorów systemów teleinformatycznych, zgodnie z określonymi procedurami;
   2) przestrzeganie obowiązujących dokumentów normatywnych, zaleceń i wytycznych w zakresie bezpieczeństwa teleinformatycznego oraz reagowania na incydenty komputerowe;
   3) realizowanie Lokalnych Procedur Operacyjnych SRnIK;
   4) nie później niż do końca 2015 r., uwzględnienie obowiązków nałożonych decyzją w dokumentacji bezpieczeństwa teleinformatycznego oraz dokumentacji eksploatacyjnej i procedurach dla systemów teleinformatycznych.
10. Traci moc decyzja Nr 243/MON Ministra Obrony Narodowej z dnia 18 czerwca 2014 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej (Dz. Urz. Min. Obr. Nar. poz. 203).
11. Decyzja wchodzi w życie z dniem ogłoszenia.

Minister Obrony Narodowej: *T. Siemoniak*