Departament Informatyki i Telekomunikacji

205

DECYZJA Nr 357/MON MINISTRA OBRONY NARODOWEJ

z dnia 29 lipca 2008 r.

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

Na podstawie § 2 pkt 6 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426), w związku z art. 2 pkt 6a ustawy z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz. U. z 1996 r. Nr 10, poz. 56, z późn. zm.[1)]) ustala się, co następuje:

§ 1. Użyte w decyzji określenia oznaczają:

1) resort obrony narodowej — dział administracji rządowej, w skład którego wchodzą: Minister jako kierownik działu administracji rządowej — obrona narodowa, Ministerstwo jako urząd, jednostki organizacyjne podległe lub nadzorowane przez Ministra, w tym przedsiębiorstwa państwowe, dla których jest on organem założycielskim oraz Siły Zbrojne Rzeczypospolitej Polskiej;
2) jednostka organizacyjna:
   a) Ministerstwo Obrony Narodowej jako urząd Ministra Obrony Narodowej,
   b) jednostka organizacyjna podległa Ministrowi Obrony Narodowej lub przez niego nadzorowana,
   c) jednostka wojskowa lub związek organizacyjny wchodzące w skład Sił Zbrojnych — w rozumieniu przepisów ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej;
3) komórka organizacyjna — komórkę organizacyjną Ministerstwa Obrony Narodowej w rozumieniu rozporządzenia Prezesa Rady Ministrów z dnia 24 października 2006 r. w sprawie nadania statutu Ministerstwu Obrony Narodowej (Dz. U. Nr 76, poz. 768, z 2007 r. Nr 57, poz. 647 oraz Nr 97, poz. 1073);
4) kierownik jednostki (komórki) organizacyjnej — dowódcę, dyrektora, szefa, komendanta, prezesa;
5) pełnomocnik ochrony — pełnomocnika kierownika jednostki organizacyjnej do spraw ochrony informacji niejawnych;
6) administrator — osobę lub zespół osób odpowiedzialnych za funkcjonowanie systemów lub sieci teleinformatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci teleinformatycznych;
7) system teleinformatyczny — system, który tworzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji;
8) sieć teleinformatyczna — organizacyjne i techniczne połączenie systemów teleinformatycznych;
9) zdarzenie — określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;
10) incydent komputerowy — pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia procesów dowodzenia i kierowania oraz zagrażają bezpieczeństwu informacji;
11) zagrożenie — potencjalną możliwość naruszenia bezpieczeństwa systemu lub sieci teleinformatycznej;
12) reagowanie — zachowanie lub postępowanie jako odpowiedź na zaistniałe zdarzenie;
13) System Reagowania na Incydenty Komputerowe resortu obrony narodowej (SRnIK) — system zorganizowany w trzypoziomową strukturę, w skład której wchodzą:
   a) Centrum Koordynacyjne, którego funkcję spełnia Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki na podstawie Decyzji Nr 24/MON z dnia 31 stycznia 2006 r. w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej (Dz. Urz. MON Nr 2, poz. 19 oraz z 2007 r. Nr 23, poz. 241),

---

[1)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1996 r. Nr 102, poz. 474, z 1997 r. Nr 121, poz. 770 i Nr 141, poz. 944, z 1999 r. Nr 11, poz. 95, z 2001 r. Nr 123, poz. 1353 i Nr 154, poz. 1800, z 2002 r. Nr 156, poz. 1301, z 2003 r. Nr 210, poz. 2036, z 2006 r. Nr 104, poz. 711 oraz z 2007 r. Nr 107, poz. 732

b) Centrum Wsparcia Technicznego, którego funkcję spełnia Centrum Zarządzania Systemami Teleinformatycznymi na podstawie Decyzji Nr 24/MON z dnia 31 stycznia 2006 r. w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej,
c) administratorzy systemów i sieci teleinformatycznych w jednostkach i komórkach organizacyjnych;

14) organizator systemu — instytucję wojskową (osobę funkcyjną) odpowiedzialną za tworzenie, rozwój i funkcjonowanie systemu.

§ 2. 1. W celu zapewnienia realizacji i koordynacji procesów zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach i sieciach teleinformatycznych resortu obrony narodowej, z wyłączeniem systemów i sieci teleinformatycznych i narodowych segmentów sieci międzynarodowych Służby Wywiadu Wojskowego i Służby Kontrwywiadu Wojskowego, organizuje się SRnIK.

2. Nadzór nad funkcjonowaniem SRnIK sprawuje Dyrektor Departamentu Informatyki i Telekomunikacji Ministerstwa Obrony Narodowej.

§ 3. Departament Informatyki i Telekomunikacji jest uprawniony i właściwy do:

1) przeprowadzania przeglądów SRnIK oraz reagowania na wyniki tych przeglądów;
2) pełnienia roli punktu kontaktowego SRnIK w stosunku do organizacji narodowych i międzynarodowych, w tym Organizacji Traktatu Północnoatlantyckiego;
3) organizowania resortowych systemów i sieci teleinformatycznych z uwzględnieniem procesów realizowanych w ramach SRnIK;
4) tworzenia polityki wykorzystania systemów i sieci teleinformatycznych resortu obrony narodowej przez inne osoby prawne i fizyczne;
5) organizowania szkoleń z zakresu reagowania na incydenty komputerowe;
6) zatwierdzania dokumentów określonych w § 7 ust. 1 pkt 1.

§ 4. Centrum Koordynacyjne SRnIK jest uprawnione i właściwe do:

1) koordynowania procesu reagowania na incydenty komputerowe w systemach i sieciach teleinformatycznych;
2) określania zasad funkcjonowania SRnIK;
3) nadzoru nad realizacją zadań przez Centrum Wsparcia Technicznego SRnIK;
4) prowadzenia działań proaktywnych, polegających na analizie infrastruktury teleinformatycznej i opracowywaniu zaleceń zapobiegających wystąpieniu incydentów;
5) współpracy w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego:
   a) z Centrum Koordynacyjnym systemu reagowania na incydenty komputerowe w Organizacji Traktatu Północnoatlantyckiego,
   b) z krajowymi i międzynarodowymi organami koordynującymi systemu reagowania na incydenty komputerowe,
   c) z Agencją Bezpieczeństwa Wewnętrznego (Rządowym Zespołem do spraw Reagowania na Incydenty Komputerowe),
   d) ze Służbą Kontrwywiadu Wojskowego,
   e) z Departamentem Ochrony Informacji Niejawnych Ministerstwa Obrony Narodowej,
   f) z Żandarmerią Wojskową,
   g) z Zarządem Planowania Systemów Dowodzenia i Łączności — P6 Sztabu Generalnego Wojska Polskiego,
   h) z pionami ochrony właściwych jednostek organizacyjnych;
6) analizowaniu informacji o zdarzeniach oraz tworzenia na ich bazie okresowych raportów o stanie bezpieczeństwa w systemach i sieciach teleinformatycznych;
7) udziału w pracach grup roboczych w ramach Organizacji Traktatu Północnoatlantyckiego oraz reprezentowania resortu obrony narodowej w kontaktach z organizacjami spoza resortu obrony narodowej w zakresie reagowania na incydenty w systemach i sieciach teleinformatycznych;
8) prowadzenia portali informacyjnych — oddzielnie dla jawnych i niejawnych sieci i systemów teleinformatycznych resortu obrony narodowej — na potrzeby obsługi incydentów komputerowych;
9) prowadzenia wykazu osób funkcyjnych odpowiedzialnych za SRnIK i osób współpracujących w tym zakresie, w tym danych teleadresowych.

§ 5. Centrum Wsparcia Technicznego Systemu Reagowania na Incydenty Komputerowe jest uprawnione i właściwe do:

1) współpracy z Centrum Koordynacyjnym SRnIK w zakresie ustalania zasad funkcjonowania SRnIK;
2) współpracy w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego:
   a) z Centrum Technicznym systemu reagowania na incydenty komputerowe Organizacji Traktatu Północnoatlantyckiego,
   b) z krajowymi i międzynarodowymi zespołami systemu reagowania na incydenty komputerowe,
   c) z pionami ochrony właściwych jednostek organizacyjnych;
3) monitorowania w trybie ciągłym stanu bezpieczeństwa systemów i sieci teleinformatycznych;

4) zbierania informacji o zdarzeniach oraz tworzenia na ich bazie raportów o stanie bezpieczeństwa w nadzorowanych systemach i sieciach teleinformatycznych;
5) prowadzenia, w porozumieniu z właściwymi pionami ochrony, kontroli konfiguracji systemów i sieci teleinformatycznych, z wykorzystaniem określonych w pkt 8 środków technicznych, w celu ustalenia aktualnego stanu zabezpieczenia tych systemów i sieci;
6) realizacji zadań związanych z bezpośrednią obsługą incydentów w systemach i sieciach teleinformatycznych;
7) udzielania pomocy administratorom w trakcie obsługi incydentu oraz przywracania funkcjonowania systemu lub sieci teleinformatycznej po zaistniałym incydencie;
8) stosowania zaakceptowanych przez organizatora systemu środków technicznych i organizacyjnych oraz narzędzi do zdalnego zarządzania i kontroli konfiguracji sieci i systemów teleinformatycznych, służących do zapobiegania, wykrywania i usuwania skutków naruszeń bezpieczeństwa;
9) wnioskowania do właściwego pionu ochrony w sprawie czasowego wyłączania lub zaniechania przetwarzania informacji w systemie lub sieci teleinformatycznej, w której stwierdzono wystąpienie incydentu komputerowego;
10) udziału w pracach grup roboczych w ramach Organizacji Traktatu Północnoatlantyckiego w zakresie reagowania na incydenty komputerowe;
11) prowadzenia ewidencji administratorów systemów i sieci teleinformatycznych, zawierającej stopień wojskowy, imię i nazwisko oraz numer telefonu, nazwę jednostki (komórki) organizacyjnej każdej osoby wyznaczonej do pełnienia funkcji administratora systemu.

§ 6. Administratorzy systemów i sieci teleinformatycznych w jednostkach i komórkach organizacyjnych są zobowiązani do:
1) przestrzegania obowiązujących dokumentów normatywnych i zaleceń w zakresie przeciwdziałania naruszeniom bezpieczeństwa systemów i sieci teleinformatycznych;
2) nadzorowania użytkowników administrowanych przez nich systemów i sieci teleinformatycznych w zakresie przestrzegania ustalonych procedur bezpieczeństwa;
3) wykonywania poleceń Centrum Wsparcia Technicznego SRnIK w zakresie przeciwdziałania wystąpieniu i reagowania na incydenty komputerowe;
4) współpracy z instytucjami określonymi w § 4 pkt 5 lit d, e, f w zakresie zabezpieczenia śladów i ustalenia przyczyn wystąpienia incydentu;
5) zgłaszania do Centrum Wsparcia Technicznego SRnIK oraz inspektora bezpieczeństwa teleinformatycznego wykrytych naruszeń bezpieczeństwa oraz wszelkich zdarzeń mogących wpłynąć na naruszenie bezpieczeństwa teleinformatycznego w administrowanych przez nich systemach i sieciach teleinformatycznych;
6) informowania Centrum Wsparcia Technicznego SRnIK o zmianach personalnych administratorów oraz istotnych zmianach w konfiguracji systemów i sieci teleinformatycznych mogących mieć wpływ na ich bezpieczeństwo.

§ 7. 1. Dyrektor Wojskowego Biura Bezpieczeństwa Łączności i Informatyki odpowiada za:
1) opracowanie i aktualizację:
   a) „Podręcznika reagowania na incydenty komputerowe w resorcie obrony narodowej”,
   b) „Standardowych Procedur Operacyjnych SRnIK w resorcie obrony narodowej”;
2) przekazanie dokumentacji określonej w ust. 1 pkt 1 do zatwierdzenia Dyrektora Departamentu Informatyki i Telekomunikacji;
3) wdrażanie w resorcie obrony narodowej zaleceń Służby Kontrwywiadu Wojskowego z zakresu bezpieczeństwa teleinformatycznego, o których mowa w art. 5 ust. 1 pkt 3 ustawy z dnia 9 czerwca 2006 r o Służbie Kontrwywiadu Wojskowego (Dz. U. Nr 104, poz. 709 oraz Nr 218, poz. 1592);

2. Dokumentacja, o której mowa w ust. 1 pkt 1, przed zatwierdzeniem podlega uzgodnieniu:
1) ze Służbą Kontrwywiadu Wojskowego;
2) z Departamentem Ochrony Informacji Niejawnych;
3) z Żandarmerią Wojskową;
4) z Centrum Zarządzania Systemami Teleinformatycznymi;
5) z Zarządem Planowania Systemów Dowodzenia i Łączności — P6 Sztabu Generalnego Wojska Polskiego.

§ 8. Kierownicy wszystkich szczebli kierowania i dowodzenia resortu zapewnią:
1) ścisłe przestrzeganie i realizowanie przez podległe stany osobowe procedur przeciwdziałania incydentom komputerowym;
2) ścisłe przestrzeganie obowiązujących dokumentów normatywnych i zaleceń w zakresie przeciwdziałania naruszeniom bezpieczeństwa systemów i sieci teleinformatycznych;
3) realizowanie przez użytkowników systemów i sieci teleinformatycznych poleceń administratora w zakresie określonym w § 6;
4) uwzględnienie obowiązków nałożonych niniejszą decyzją w dokumentacji bezpieczeństwa systemów i sieci teleinformatycznych.

§ 9.1. Powołuje się Zespół do prowadzenia cyklicznych analiz zagrożeń dla przetwarzania w systemach i sieciach teleinformatycznych, w tym m.in. określania przyczyn wystąpienia incydentów komputerowych oraz sposobów postępowania zapobiegających występowaniu ich w przyszłości, zwany dalej „Zespołem”.

2. W skład Zespołu wchodzą przedstawiciele: Departamentu Informatyki i Telekomunikacji, Departamentu Ochrony Informacji Niejawnych, Komendy Głównej Żandarmerii Wojskowej, Służby Kontrwywiadu Wojskowego, Zarządu Planowania Systemów Dowodzenia i Łączności — P6 Sztabu Generalnego Wojska Polskiego, Centrum Zarządzania Systemami Teleinformatycznymi oraz Wojskowego Biura Bezpieczeństwa Łączności i Informatyki.

3. Przewodniczącego Zespołu wyznaczy Dyrektor Departamentu Informatyki i Telekomunikacji.

4. Kierownicy jednostek organizacyjnych, wymienionych w ust. 2, przedstawią Dyrektorowi Departamentu Informatyki i Telekomunikacji imienne kandydatury członków Zespołu — w terminie nie dłuższym, niż 14 dni po wejściu decyzji w życie.

5. Przewodniczący Zespołu zwołuje jego posiedzenia nie rzadziej niż raz na trzy miesiące.

§ 10. Decyzja wchodzi w życie z dniem ogłoszenia.

Minister Obrony Narodowej: *B. Klich*