(Akty przyjęte na mocy Tytułu VI Traktatu o Unii Europejskiej)

DECYZJA RAMOWA RADY 2005/222/WSiSW

z dnia 24 lutego 2005 r.

w sprawie ataków na systemy informatyczne

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o Unii Europejskiej, a w szczególności jego art. 29, art. 30 ust. 1 lit. a), art. 31 ust. 1 lit. e) i art. 34 ust. 2 lit. b),

uwzględniając wniosek Komisji,

uwzględniając opinię Parlamentu Europejskiego [1],

a także mając na uwadze, co następuje:

(1) Celem niniejszej decyzji ramowej jest usprawnienie współpracy między organami sądowymi i innymi właściwymi organami, włącznie z policją i innymi wyspecjalizowanymi organami ścigania Państw Członkowskich, poprzez zbliżanie zasad prawa karnego w Państwach Członkowskich w dziedzinie ataków na systemy informatyczne.

(2) Istnieją dowody ataków na systemy informatyczne, w szczególności w wyniku zagrożenia przestępczością zorganizowaną, rosną także obawy spowodowane możliwymi atakami terrorystycznymi na systemy informatyczne, które stanowią część mającej istotne znaczenie infrastruktury Państw Członkowskich. Stanowi to zagrożenie dla osiągnięcia bardziej bezpiecznego społeczeństwa informacyjnego oraz przestrzeni wolności, bezpieczeństwa i sprawiedliwości, a zatem wymaga reakcji na poziomie Unii Europejskiej.

(3) Skuteczna reakcja na te zagrożenia wymaga wszechstronnego podejścia do bezpieczeństwa sieci i informacji, jak podkreślono w planie działań *e*Europa, w komunikacie Komisji „Bezpieczeństwo sieci i informacji: Propozycje na rzecz europejskiego podejścia" oraz w rezolucji Rady z dnia 28 stycznia 2002 r. w sprawie wspólnego podejścia i działań szczególnych w dziedzinie bezpieczeństwa sieci i informacji [2].

(4) Potrzeba dalszego podniesienia poziomu świadomości dotyczącej problemów związanych z bezpieczeństwem informacji oraz zapewnienia praktycznej pomocy została również podkreślona w rezolucji Parlamentu Europejskiego z dnia 5 września 2001 r.

(5) Istotne luki i różnice w przepisach prawnych Państw Członkowskich w tej dziedzinie mogą utrudniać walkę z przestępczością zorganizowaną i terroryzmem oraz mogą komplikować skuteczną współpracę policyjną i sądową w dziedzinie ataków na systemy informatyczne. Transnarodowy i ponadgraniczny charakter nowoczesnych systemów informatycznych oznacza, że ataki na takie systemy mają często charakter transgraniczny, co podkreśla pilną potrzebę dalszego działania w celu zbliżania ustawodawstw karnych w tej dziedzinie.

(6) Rada i Komisja w planie działań w sprawie najlepszego sposobu wykonania postanowień Traktatu z Amsterdamu w dziedzinie przestrzeni wolności, bezpieczeństwa i sprawiedliwości [3], Rada Europejska na posiedzeniu w Tampere w dniach 15 i 16 października 1999 r., Rada Europejska na posiedzeniu w Santa Maria de Feira w dniach 19 i 20 czerwca 2000 r., Komisja w „Zestawieniu wyników" oraz Parlament Europejski w swojej rezolucji z 19 maja 2000 r. wskazują lub wzywają do podjęcia działań legislacyjnych przeciwko przestępczości z wykorzystaniem zaawansowanej technologii, w tym do ustanowienia wspólnych definicji, przestępstw i sankcji.

(7) Należy uzupełnić pracę wykonywaną przez organizacje międzynarodowe, w szczególności pracę Rady Europy w zakresie zbliżania prawa karnego oraz pracę grupy G8 w zakresie współpracy transgranicznej w dziedzinie przestępczości z wykorzystaniem zaawansowanej technologii, poprzez ustanowienie w tej dziedzinie wspólnego podejścia w Unii Europejskiej. Wezwanie to zostało rozwinięte w komunikacie Komisji adresowanym do Rady, Parlamentu Europejskiego, Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów w sprawie „Tworzenia bardziej bezpiecznego społeczeństwa informacyjnego poprzez ulepszanie bezpieczeństwa infrastruktury informatycznej oraz zwalczania przestępczości komputerowej".

(8) Należy zbliżyć prawo karne w dziedzinie ataków na systemy informatyczne w celu zapewnienia współpracy policyjnej i sądowej o najszerszym możliwym zakresie w dziedzinie przestępstw związanych z atakami na systemy informatyczne oraz aby przyczynić się do walki z przestępczością zorganizowaną i terroryzmem.

[1] Dz.U. C 300 E z 11.12.2003, str. 26.
[2] Dz.U. C 43 z 16.2.2002, str. 2.
[3] Dz.U. C 19 z 23.1.1999, str. 1.

(9) Wszystkie Państwa Członkowskie ratyfikowały Konwencję Rady Europy z 28 stycznia 1981 r. o ochronie osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych. Dane osobowe przetwarzane podczas wprowadzania w życie niniejszej decyzji ramowej powinny być chronione zgodnie z zasadami powyższej Konwencji.

(10) Wspólne definicje w tej dziedzinie, szczególnie definicje systemów informatycznych i danych komputerowych są istotne, aby zapewnić spójne podejście w Państwach Członkowskich przy stosowaniu niniejszej decyzji ramowej.

(11) Istnieje potrzeba osiągnięcia wspólnego podejścia w odniesieniu do znamion przestępstw poprzez wspólne określenie przestępstw nielegalnego dostępu do systemu informatycznego, nielegalnej ingerencji w system informatyczny i nielegalnej ingerencji w dane.

(12) W interesie zwalczania przestępczości komputerowej każde Państwo Członkowskie powinno zapewnić skuteczną współpracę sądową w odniesieniu do przestępstw opartych na rodzajach zachowań, o których mowa w art. 2, 3, 4 i 5.

(13) Istnieje potrzeba uniknięcia nadmiernej kryminalizacji, szczególnie w przypadkach mniejszej wagi, jak również potrzeba uniknięcia kryminalizacji posiadaczy praw i osób upoważnionych.

(14) Istnieje potrzeba ustanowienia przez Państwa Członkowskie sankcji za ataki na systemy informatyczne. Przewidziane sankcje powinny być skuteczne, proporcjonalne i odstraszające.

(15) Ustanowienie bardziej dotkliwych sankcji jest właściwe, jeżeli atak na system informatyczny został dokonany w ramach organizacji przestępczej, zdefiniowanej we wspólnym działaniu 98/733/WSiSW z dnia 21 grudnia 1998 r. w sprawie uznawania za przestępstwa karne uczestnictwa w organizacji przestępczej w Państwach Członkowskich Unii Europejskiej [1]. Ustanowienie bardziej dotkliwych sankcji jest również właściwe w przypadkach, kiedy taki atak spowodował poważne szkody lub miał wpływ na istotne interesy.

(16) Należy również przewidzieć środki służące współpracy między Państwami Członkowskimi, mając na względzie zapewnienie skutecznego działania przeciwko atakom na systemy informatyczne. Do celów wymiany informacji Państwa Członkowskie powinny zatem korzystać z istniejącej sieci operacyjnych punktów kontaktowych, o których mowa w zaleceniu Rady z dnia 25 czerwca 2001 r. w sprawie punktów kontaktowych utrzymujących 24-godzinny dyżur w celu zwalczania przestępczości z wykorzystaniem zaawansowanej technologii [2].

(17) Ponieważ cele niniejszej decyzji ramowej, czyli zapewnienie, że we wszystkich Państwach Członkowskich ataki na systemy informatyczne są zagrożone skutecznymi, proporcjonalnymi i odstraszającymi sankcjami karnymi oraz usprawnianie i zachęcanie do współpracy sądowej poprzez usuwanie potencjalnych przeszkód, nie mogą być w sposób wystarczający osiągnięte przez Państwa Członkowskie w związku z tym, że zasady muszą być wspólne i kompatybilne, natomiast możliwe jest lepsze osiągnięcie tych celów na poziomie Unii, Unia może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu WE. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza decyzja ramowa nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(18) Niniejsza decyzja ramowa szanuje prawa podstawowe i przestrzega zasad uznanych w art. 6 Traktatu o Unii Europejskiej oraz odzwierciedlonych w Karcie Praw Podstawowych Unii Europejskiej, w szczególności w jej rozdziałach II i VI,

PRZYJMUJE NINIEJSZĄ DECYZJĘ RAMOWĄ:

Artykuł 1

Definicje

Do celów niniejszej decyzji ramowej stosuje się następujące definicje:

a) „system informatyczny" oznacza wszelkie urządzenia lub grupę połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych komputerowych, jak również danych przechowywanych, przetwarzanych, odzyskanych lub przekazanych przez nie w celach ich eksploatacji, użycia, ochrony lub utrzymania;

b) „dane komputerowe" oznaczają wszelkie przedstawienie faktów, informacji lub koncepcji w formie odpowiedniej do przetwarzania w systemie informatycznym, włącznie z programem odpowiednim do spowodowania wykonania funkcji przez system;

c) „osoba prawna" oznacza wszelkie podmioty mające taki status na mocy właściwego prawa, z wyjątkiem organów państwowych lub innych organów publicznych wykonujących władzę państwową oraz publicznych organizacji międzynarodowych;

[1] Dz.U. L 351 z 29.12.1998, str. 1.

[2] Dz.U. C 187 z 3.7.2001, str. 5.

d) „bezprawne" oznacza dostęp lub ingerencję, na którą właściciel, inny posiadacz prawa do systemu lub jego części nie udzielił zgody lub która nie jest dozwolona na mocy prawa krajowego.

Artykuł 2

Nielegalny dostęp do systemów informatycznych

1. Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że umyślny bezprawny dostęp do całości lub części systemu informatycznego jest karalny jako przestępstwo, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.

2. Każde Państwo Członkowskie może zdecydować, że zachowanie, o którym mowa w ust. 1 jest objęte oskarżeniem jedynie w przypadkach, kiedy przestępstwo popełniane jest z naruszeniem zabezpieczenia.

Artykuł 3

Nielegalna ingerencja w system

Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że umyślne poważne naruszenie lub przerwanie funkcjonowania systemu informatycznego poprzez wprowadzanie, przekazywanie, uszkadzanie, usuwanie, niszczenie, zmienianie, zatajanie lub uczynienie niedostępnymi danych komputerowych jest karalne jako przestępstwo, kiedy dokonane jest bezprawnie, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.

Artykuł 4

Nielegalna ingerencja w dane

Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że umyślne bezprawne usunięcie, uszkodzenie, pogorszenie, zmiana, zatajanie lub uczynienie niedostępnymi danych komputerowych w systemie informatycznym jest karane jako przestępstwo, kiedy dokonywane jest bezprawnie, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.

Artykuł 5

Kierowanie, pomaganie i podżeganie oraz usiłowanie

1. Każde Państwo Członkowskie zapewnia, że kierowanie, pomaganie i podżeganie do przestępstw, o których mowa w art. 2, 3 i 4, jest karane jak przestępstwo.

2. Każde Państwo Członkowskie zapewnia, że usiłowanie popełnienia przestępstw, o których mowa w art. 2, 3 i 4, jest karane jak przestępstwo.

3. Każde Państwo Członkowskie może zdecydować o niestosowaniu ustępu 2 do przestępstw, o których mowa w art. 2.

Artykuł 6

Sankcje

1. Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że przestępstwa, o których mowa w art. 2, 3, 4 i 5, podlegają skutecznym, proporcjonalnym i odstraszającym sankcjom karnym.

2. Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że przestępstwa, których mowa w art. 3 i 4, podlegają karze do wysokości przynajmniej od 1 roku do 3 lat pozbawienia wolności.

Artykuł 7

Okoliczności obciążające

1. Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że przestępstwo, o którym mowa w art. 2 ust. 2, oraz przestępstwo, o którym mowa w art. 3 i 4, podlegają karze do wysokości przynajmniej od 2 do 5 lat pozbawienia wolności, jeżeli popełnione zostały w ramach organizacji przestępczej określonej we wspólnym działaniu 98/733/WSiSW, z wyjątkiem poziomu sankcji, o którym w nim mowa.

2. Państwo Członkowskie może również podjąć środki, o których mowa w ust. 1, jeżeli przestępstwo spowodowało poważne szkody lub miało wpływ na istotne interesy.

Artykuł 8

Odpowiedzialność osób prawnych

1. Każde Państwo Członkowskie podejmuje niezbędne kroki celem zapewnienia, że osoba prawna może zostać pociągnięta do odpowiedzialności za przestępstwa, o których mowa w art. 2, 3, 4 i 5, które popełnione zostały z przysporzeniem jej korzyści przez jakąkolwiek osobę działającą indywidualnie lub jako część organu tej osoby prawnej, która ma ważną pozycję w tej osobie prawnej, poprzez:

a) prawo do reprezentowania osoby prawnej; lub

b) uprawnienie do podejmowania decyzji w imieniu osoby prawnej; lub

c) uprawnienie do sprawowania kontroli w ramach osoby prawnej.

2. Oprócz przypadków, o których mowa w ust. 1, Państwa Członkowskie zapewniają, że osoba prawna może zostać pociągnięta do odpowiedzialności, w przypadku gdy brak nadzoru lub kontroli przez osobę, o której mowa w ust. 1, umożliwił popełnienie przestępstw, o których mowa w art. 2, 3, 4 i 5, z przysporzeniem korzyści tej osobie prawnej przez osobę pozostającą pod jej władzą.

3. Odpowiedzialność osoby prawnej na podstawie ust. 1 i 2 nie wyklucza postępowania karnego przeciwko osobom fizycznym, które jako sprawca, podżegacz lub pomocnik mają związek z popełnieniem przestępstw, o których mowa w art. 2, 3, 4 i 5.

Artykuł 9

Sankcje wobec osób prawnych

1. Każde Państwo Członkowskie podejmuje niezbędne kroki celem zapewnienia, że osoba prawna uznana za odpowiedzialną na podstawie art. 8 ust. 1 podlega skutecznym, proporcjonalnym i odstraszającym sankcjom karnym, obejmującym kary grzywny i kary finansowe oraz mogącym obejmować inne sankcje, w tym:

a) wyłączenie z uprawnienia do przywilejów lub pomocy publicznej;

b) czasowy lub stały zakaz prowadzenia działalności gospodarczej;

c) umieszczenie pod nadzorem sądowym; lub

d) sądowy nakaz likwidacji.

2. Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że osoba prawna uznana za odpowiedzialną zgodnie z art. 8 ust. 2 podlega skutecznym, proporcjonalnym lub odstraszającym sankcjom lub środkom.

Artykuł 10

Jurysdykcja

1. Każde Państwo Członkowskie ustanawia swoją jurysdykcję w sprawie przestępstw, o których mowa w art. 2, 3, 4 i 5, jeżeli przestępstwo zostało popełnione:

a) w całości lub częściowo na jego terytorium; lub

b) przez jednego z jego obywateli; lub

c) z przysporzeniem korzyści osobie prawnej, której siedziba znajduje się na terytorium tego Państwa Członkowskiego.

2. Ustanawiając jurysdykcję zgodnie z ust. 1 lit. a), każde Państwo Członkowskie zapewnia, że jurysdykcja obejmuje przypadki, gdzie:

a) sprawca popełnia przestępstwo znajdując się na jego terytorium, niezależnie od tego, czy przestępstwo jest skierowane przeciwko systemowi informatycznemu na jego terytorium; lub

b) przestępstwo jest skierowane przeciwko systemowi informatycznemu na jego terytorium, niezależnie od tego, czy sprawca popełnia przestępstwo znajdując się na jego terytorium.

3. Państwo Członkowskie, które zgodnie ze swoim prawem nie dokonuje na razie ekstradycji lub przekazania swoich obywateli podejmuje niezbędne środki celem ustanowienia nad nimi jurysdykcji oraz ścigania, tam gdzie jest to właściwe, przestępstw, o których mowa w art. 2, 3, 4 i 5, jeżeli zostały popełnione przez jego obywatela poza terytorium tego Państwa Członkowskiego.

4. Jeżeli przestępstwo podlega jurysdykcji więcej niż jednego Państwa Członkowskiego i jeżeli każde z zainteresowanych Państw może je skutecznie ścigać na podstawie tych samych faktów, zainteresowane Państwa Członkowskie współpracują w celu zdecydowania, które z nich będzie ścigać sprawców z zamiarem, jeżeli jest to możliwe, scentralizowania postępowania w jednym Państwie Członkowskim. W tym celu Państwa Członkowskie mogą zwrócić się do jakiegokolwiek organu lub skorzystać z mechanizmu ustanowionego w ramach Unii Europejskiej w celu ułatwienia współpracy między ich organami sądowymi i koordynacji ich działań. Bierze się pod uwagę kolejno następujące okoliczności:

— Państwo Członkowskie jest tym, na terytorium którego popełniono przestępstwa, zgodnie z ust. 1 lit. a) i ust. 2,

— Państwo Członkowskie jest tym, którego obywatel jest sprawcą,

— Państwo Członkowskie jest tym, w którym odnaleziono sprawcę.

5. Państwo Członkowskie może zdecydować o niestosowaniu lub stosowaniu jedynie w szczególnych przypadkach lub okolicznościach zasad dotyczących jurysdykcji określonych w ust. 1 lit. b) i ust. 1 lit. c).

6. Państwa Członkowskie informują Sekretariat Generalny Rady i Komisję, jeżeli zdecydują się na stosowanie ust. 5, tam gdzie jest to właściwe, wskazując szczególne przypadki lub okoliczności, do których decyzja ta ma zastosowanie.

Artykuł 11

Wymiana informacji

1. Do celów wymiany informacji odnoszących się do przestępstw, o których mowa w art. 2, 3, 4 i 5 oraz zgodnie z zasadami ochrony danych, Państwa Członkowskie zapewniają, że korzystają z istniejącej sieci operacyjnych punktów kontaktowych dostępnych 24 godziny na dobę oraz przez siedem dni w tygodniu.

2. Każde Państwo Członkowskie informuje Sekretariat Generalny Rady oraz Komisję o swoich wyznaczonych punktach kontaktowych do celów wymiany informacji dotyczących ataków na systemy informatyczne. Sekretariat Generalny przekazuje takie informacje innym Państwom Członkowskim.

Artykuł 12

Wprowadzenie w życie

1. Państwa Członkowskie podejmują niezbędne środki w celu stosowania przepisów niniejszej decyzji ramowej do 16 marca 2007 r.

2. Do 16 marca 2007 r. Państwa Członkowskie przekażą Sekretariatowi Generalnemu Rady oraz Komisji teksty wszelkich przepisów przenoszących do ich prawa krajowego obowiązki nałożone na nie na podstawie niniejszej decyzji ramowej. Do 16 września 2007 r., w oparciu o sprawozdanie sporządzone na podstawie informacji i pisemnego sprawozdania Komisji, Rada oceni stopień, do którego Państwa Członkowskie zastosowały się do przepisów niniejszej decyzji ramowej.

Artykuł 13

Wejście w życie

Niniejsza decyzja ramowa wchodzi w życie w dniu jej opublikowania w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli, dnia 24 lutego 2005 r.

W imieniu Rady
N. SCHMIT
Przewodniczący