DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY 2013/40/UE

z dnia 12 sierpnia 2013 r.

dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 83 ust. 1,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ([1]),

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([2]),

a także mając na uwadze, co następuje:

(1) Celami niniejszej dyrektywy są: zbliżenie prawa karnego państw członkowskich w dziedzinie ataków na systemy informatyczne, przez ustanowienie zasad minimalnych dotyczących definicji przestępstw i odpowiednich kar, oraz poprawa współpracy między właściwymi organami, w tym policją i innymi wyspecjalizowanymi organami ścigania w państwach członkowskich, a także właściwymi wyspecjalizowanymi agencjami i organami Unii takimi jak Eurojust, Europol i należące do niego Europejskie Centrum ds. Walki z Cyberprzestępczością oraz Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA).

(2) Systemy informatyczne stanowią podstawowy element relacji politycznych, społecznych i gospodarczych w Unii. Zależność społeczeństwa od tego typu systemów jest bardzo wysoka i stale rośnie. Dobre funkcjonowanie i bezpieczeństwo tych systemów w Unii są niezbędne dla rozwoju rynku wewnętrznego oraz konkurencyjnej i innowacyjnej gospodarki. Zapewnianie odpowiedniego poziomu ochrony systemów informatycznych powinno być realizowane w ramach ogółu skutecznych i kompleksowych środków profilaktycznych, jakie towarzyszą działaniom wobec cyberprzestępczości podejmowanym w obszarze prawa karnego.

(3) Zarówno na obszarze Unii, jak i globalnie, rośnie zagrożenie atakami na systemy informatyczne, a zwłaszcza atakami dokonywanymi w ramach przestępczości zorganizowanej; narastają również obawy o możliwość ataków o charakterze terrorystycznym lub mających podłoże polityczne, ukierunkowanych na systemy informatyczne stanowiące element infrastruktury krytycznej państw członkowskich i Unii. Zagraża to dążeniom do zapewnienia bezpieczniejszego społeczeństwa informacyjnego oraz przestrzeni wolności, bezpieczeństwa i sprawiedliwości, dlatego też wymaga reakcji na szczeblu Unii, a także lepszej współpracy i koordynacji na szczeblu międzynarodowym.

(4) Na obszarze Unii znajduje się szereg infrastruktur krytycznych, których zakłócenie lub zniszczenie miałoby istotne transgraniczne skutki. Z potrzeby wzmocnienia zdolności ochrony infrastruktury krytycznej w Unii jasno wynika, że środkom wymierzonym przeciw atakom cybernetycznym powinny towarzyszyć surowe sankcje karne odzwierciedlające wagę tych ataków. Infrastrukturę krytyczną można rozumieć jako składnik, system lub część infrastruktury zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności, jak na przykład elektrownie, sieci transportowe lub sieci rządowe, a których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku niezdolności do utrzymania tych funkcji.

(5) Istnieją dowody wskazujące na tendencję do coraz bardziej niebezpiecznych i ponawianych ataków na wielką skalę dokonywanych na systemy informatyczne, które często mają zasadnicze znaczenie dla państw członkowskich lub poszczególnych funkcji w sektorze publicznym lub prywatnym. Tendencja ta występuje wraz z opracowywaniem coraz bardziej wyrafinowanych metod takich jak tworzenie i wykorzystywanie tzw. „botnetów", co odbywa się na kilku etapach działania przestępczego, przy czym każdy z tych etapów z osobna może stanowić poważne ryzyko dla interesu publicznego. Niniejsza dyrektywa ma na celu m.in. wprowadzenie sankcji karnych za tworzenie „botnetów" - tj. działań polegających na uzyskaniu zdalnej kontroli nad znaczną liczbą komputerów przez wprowadzenie do nich złośliwego oprogramowania za pomocą ukierunkowanych cyberataków. Następnie zainfekowaną sieć komputerów stanowiącą „botnet" można uruchomić bez wiedzy użytkowników komputerów, aby rozpocząć cyberataki na wielką skalę, które zazwyczaj mogą spowodować poważne szkody, o czym mowa w niniejszej dyrektywie. Państwa członkowskie mogą określić, co, zgodnie z ich prawem krajowym oraz praktykami krajowymi, stanowi poważną szkodę, np. zakłócenie usług systemowych o dużym znaczeniu publicznym lub spowodowanie znacznych kosztów finansowych lub też utrata danych osobowych lub informacji szczególnie chronionych.

(6) Cyberataki na dużą skalę mogą powodować znaczne szkody w gospodarce zarówno przez zakłócanie pracy systemów informatycznych i łączności, jak i przez utratę lub modyfikację istotnych z handlowego punktu widzenia informacji poufnych lub innych danych. Szczególną uwagę należy zwrócić na uświadamianie innowacyjnych małych i średnich przedsiębiorstw o zagrożeniach związanych z takimi atakami i ich podatności na nie z racji ich wzrastającego uzależnienia od właściwego funkcjonowania i dostępności systemów informatycznych oraz często ograniczonych zasobów przeznaczanych na bezpieczeństwo informatyczne.

([1]) Dz.U. C 218 z 23.7.2011, s. 130.

([2]) Stanowisko Parlamentu Europejskiego z dnia 4 lipca 2013 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 22 lipca 2013 r.

(7) Wspólne definicje w tej dziedzinie mają istotne znaczenie dla zagwarantowania przyjęcia przez państwa członkowskie spójnego podejścia do stosowania niniejszej dyrektywy.

(8) Zachodzi potrzeba zapewnienia wspólnego podejścia do kwestii znamion przestępstwa poprzez powszechne wprowadzenie pojęcia przestępstw polegających na bezprawnym dostępie do systemu informatycznego, bezprawnym ingerowaniu w system, bezprawnym ingerowaniu w dane oraz bezprawnym przechwytywaniu.

(9) Przechwytywanie odnosi się między innymi, lecz nie wyłącznie, do słuchania, monitorowania lub nadzorowania treści komunikatów, do pozyskiwania treści danych bezpośrednio poprzez dostęp do systemu informatycznego i korzystanie z niego albo pośrednio poprzez stosowanie - przy użyciu środków technicznych - elektronicznego podsłuchu lub urządzeń podsłuchowych.

(10) Państwa członkowskie powinny przewidzieć kary za ataki na systemy informatyczne. Kary te powinny być skuteczne, proporcjonalne i odstraszające i powinny obejmować karę pozbawienia wolności lub karę grzywny.

(11) Niniejsza dyrektywa przewiduje kary co najmniej w przypadkach, które nie są przypadkami mniejszej wagi. Państwa członkowskie mogą określić, co stanowi przypadek mniejszej wagi zgodnie ze swoimi przepisami krajowymi i praktyką krajową. Można uznać, że przypadek ma mniejszą wagę, jeżeli na przykład szkody wyrządzone w wyniku przestępstwa lub zagrożenie w odniesieniu do interesów publicznych lub prywatnych, takich jak integralność systemu komputerowego lub danych komputerowych lub nienaruszalność praw lub innych dóbr danej osoby, są nieznaczne lub mają taki charakter, że nałożenie sankcji karnej w przewidzianych prawnie granicach lub pociągnięcie do odpowiedzialności karnej nie jest konieczne.

(12) Stwierdzanie i zgłaszanie zagrożeń i ryzyka stwarzanych przez cyberataki oraz związanych z tym słabych punktów systemów informatycznych jest istotnym elementem skutecznego zapobiegania cyberatakom i reakcji na nie oraz polepszania bezpieczeństwa systemów informatycznych. Lepszą skuteczność zapewnić można przez zachęcanie do zgłaszania luk w systemach ochrony. Państwa członkowskie powinny czynić starania w celu stwarzania możliwości legalnego wykrywania i zgłaszania luk w systemach ochrony.

(13) Należy przewidzieć surowsze kary za ataki na systemy informatyczne popełniane przez organizację przestępczą, w rozumieniu decyzji ramowej Rady 2008/841/WSiSW z dnia 24 października 2008 r. w sprawie zwalczania przestępczości zorganizowanej [1], za cyberataki przeprowadzane na wielką skalę, wpływające zatem na dużą liczbę systemów informatycznych, w tym mające na celu stworzenie „botnetu", lub za cyberataki powodujące poważne szkody, w tym przeprowadzane z wykorzystaniem „botnetu". Właściwe jest także przewidzenie surowszych kar w przypadkach gdy atak został przypuszczony na infrastrukturę krytyczną państwa członkowskiego lub Unii.

(14) Tworzenie skutecznych środków przeciwko kradzieży tożsamości i innym przestępstwom związanym z tożsamością stanowi kolejny ważny element zintegrowanego podejścia do walki z cyberprzestępczością. Każdą potrzebę działania ze strony Unii przeciw tego rodzaju przestępczości można byłoby rozważać także w kontekście oceniania potrzeby utworzenia kompleksowego, horyzontalnego instrumentu unijnego.

(15) W konkluzjach Rady z dnia 27–28 listopada 2008 r. zaznaczono, że Komisja powinna wraz z państwami członkowskimi opracować nową strategię z uwzględnieniem treści Konwencji Rady Europy z 2001 r. o cyberprzestępczości. Konwencja ta wyznacza prawne ramy odniesienia dla zwalczania cyberprzestępczości, w tym ataków na systemy informatyczne. Niniejsza dyrektywa opiera się na tej konwencji. Możliwie najszybsze zakończenie procesu ratyfikacji konwencji przez wszystkie państwa członkowskie powinno być uważane za kwestię priorytetową.

(16) Ze względu na to, że ataki mogą być przeprowadzane na różne sposoby oraz uwzględniając szybki rozwój sprzętu i oprogramowania, w niniejszej dyrektywie mowa jest o narzędziach, które mogą zostać wykorzystane do popełnienia przestępstw w niej ustanowionych. Narzędziami tymi są przykładowo złośliwe oprogramowanie, w tym oprogramowanie zdolne do tworzenia botnetów, wykorzystywanych do przeprowadzania cyberataków. Nawet jeśli tego rodzaju narzędzie jest zdatne lub szczególnie zdatne do dokonania jednego z przestępstw ustanowionych w niniejszej dyrektywie, mogło ono jednak zostać produkowane w celach legalnych. Aby nie dopuścić do kryminalizacji przypadków produkowania takich narzędzi i wprowadzania ich na rynek w celach zgodnych z prawem - takich jak testowanie niezawodności produktów informatycznych lub bezpieczeństwa systemów informatycznych - musi być spełniony wymóg istnienia ogólnego, lecz także bezpośredniego zamiaru wykorzystania tych narzędzi do popełnienia jednego lub więcej przestępstw, ustanowionych w niniejszej dyrektywie.

(17) Celem niniejszej dyrektywy nie jest przypisanie odpowiedzialności karnej, w przypadku gdy zostały spełnione obiektywne kryteria przestępstw ustanowionych w niniejszej dyrektywie, ale czyny te popełnione zostały bez przestępczego zamiaru, np. gdy dana osoba nie wie, że dostęp jest niedozwolony lub w przypadku uzasadnionego testowania lub zabezpieczania systemów informatycznych, np. w przypadku gdy danej osobie spółka lub sprzedający zleca testowanie wytrzymałości swego systemu zabezpieczeń. W ramach niniejszej dyrektywy zobowiązania lub uzgodnienia umowne mające na celu ograniczenie dostępu do systemów informatycznych w drodze polityki użytkowników lub zasad świadczenia usługi, a także spory między pracodawcą a pracownikami co do dostępu do systemów informatycznych pracodawcy i ich użytkowania do celów prywatnych nie powinny pociągać za sobą odpowiedzialności karnej, gdy dostęp w takich sytuacjach byłby uznawany za nieupoważniony, a zatem stanowiłby wyłączną podstawę do wszczęcia postępowania karnego. Niniejsza dyrektywa nie narusza prawa dostępu do informacji określonego w ustawodawstwie krajowym i unijnym, nie może jednak służyć jako uzasadnienie bezprawnego lub arbitralnego dostępu do informacji.

[1] Dz.U. L 300 z 11.11.2008, s. 42.

(18) Dokonywanie cyberataków może być ułatwione przez różne okoliczności, takie jak sytuacja, w której sprawca w ramach stosunku pracy ma dostęp do systemów zabezpieczeń wkomponowanych w systemy informatyczne. Na podstawie prawa krajowego takie okoliczności należy odpowiednio brać pod uwagę w trakcie postępowania karnego.

(19) Państwa członkowskie powinny wprowadzić do swego prawa krajowego okoliczności obciążające – zgodnie z obowiązującymi przepisami dotyczącymi okoliczności obciążających istniejącymi w ich systemie prawnym. Państwa członkowskie powinny zapewnić, aby sędziowie mogli rozważyć te okoliczności obciążające przy skazywaniu przestępców. Ocena tych okoliczności wraz z innymi faktami danej sprawy należy do zakresu uznania sędziego.

(20) Niniejsza dyrektywa nie reguluje warunków sprawowania jurysdykcji w sprawie któregokolwiek z przestępstw w niej wymienionych, jak np. zawiadomienia złożonego przez pokrzywdzonego w miejscu popełnienia przestępstwa lub powiadomienia z państwa miejsca popełnienia przestępstwa, lub odstąpienie od ścigania sprawcy w miejscu popełnienia przestępstwa.

(21) W ramach niniejszej dyrektywy państwa i organy publiczne są w pełni zobowiązane do zagwarantowania poszanowania praw człowieka i podstawowych wolności, zgodnie z aktualnymi zobowiązaniami międzynarodowymi.

(22) Niniejsza dyrektywa zwiększa znaczenie sieci, takich jak G8 lub sieć całodobowych punktów kontaktowych Rady Europy działających siedem dni w tygodniu. Takie punkty kontaktowe powinny być w stanie udzielać skutecznej pomocy, ułatwiając tym samym np. wymianę dostępnych istotnych informacji oraz udzielanie porad technicznych lub informacji prawnych do celów dochodzenia lub postępowania w sprawach przestępstw związanych z systemami informatycznymi i powiązanymi danymi dotyczącymi państwa członkowskiego występującego z wnioskiem. Aby zapewnić niezakłócone działanie sieci, każdy punkt kontaktowy powinien być w stanie nawiązać łączność z podobnym punktem w innym państwie członkowskim szybko i z pomocą m.in. wyszkolonego i odpowiednio wyposażonego personelu. Ze względu na to, że cyberataki na wielką skalę można przeprowadzić bardzo szybko, państwa członkowskie powinny być zdolne do szybkiego reagowania na wnioski składane w trybie pilnym w ramach tej sieci punktów kontaktowych. W takich przypadkach może być zasadne, by wniosek o informacje był poparty kontaktem telefonicznym w celu zagwarantowania szybkiego przetworzenia wniosku przez państwo członkowskie, do którego wystąpiono, oraz przekazania informacji zwrotnych w ciągu ośmiu godzin.

(23) Ogromne znaczenie dla zapobiegania atakom na systemy informatyczne i zwalczania takich ataków ma współpraca organów publicznych, z jednej strony, z sektorem prywatnym i społeczeństwem obywatelskim, z drugiej. Konieczne jest wspieranie i polepszanie współpracy między dostawcami usług, producentami, organami ścigania i organami sądowymi, jednocześnie przestrzegając zasady praworządności. Współpraca taka mogłaby obejmować np. pomoc ze strony dostawców usług w zabezpieczaniu potencjalnych dowodów, w przekazywaniu informacji pomocnych w identyfikacji sprawców oraz, jako ostateczność, w wyłączaniu w całości lub w części, zgodnie z prawem krajowym i krajową praktyką w tym zakresie, systemów informatycznych lub funkcji, które zostały naruszone lub wykorzystane w celach niezgodnych z prawem. Państwa członkowskie powinny także rozważyć utworzenie sieci współpracy i partnerstwa z dostawcami usług i producentami w celu wymiany informacji związanych z przestępstwami ujętymi w niniejszej dyrektywie.

(24) Istnieje potrzeba gromadzenia porównywalnych danych o przestępstwach ustanowionych w niniejszej dyrektywie. Dane te powinny być udostępniane właściwym wyspecjalizowanym agencjom i organom Unii, takim jak Europol oraz ENISA, zgodnie z ich zakresem zadań i potrzebami informacyjnymi, by uzyskać bardziej kompletny obraz problemu cyberprzestępczości oraz poziomu bezpieczeństwa sieci i informacji na szczeblu Unii, a tym samym przyczynić się do opracowania skuteczniejszych reakcji. Państwa członkowskie powinny przekazywać Europolowi i należącemu do niego Europejskiemu Centrum ds. Walki z Cyberprzestępczością informacje o metodach działania stosowanych przez przestępców, by organy te mogły prowadzić oceny zagrożeń i strategiczne analizy cyberprzestępczości zgodnie z decyzją Rady 2009/371/WSiSW z dnia 6 kwietnia 2009 r. ustanawiającą Europejski Urząd Policji (Europol) ([1]). Przekazywanie informacji może ułatwić lepsze zrozumienie obecnych i przyszłych zagrożeń, a tym samym przyczynić się do lepszego i ukierunkowanego podejmowania decyzji dotyczących zwalczania ataków na systemy informatyczne i zapobiegania takim atakom.

(25) Zgodnie z niniejszą dyrektywą Komisja powinna przedłożyć sprawozdanie z jej stosowania oraz przedstawić wszelkie niezbędne wnioski ustawodawcze, które powodowałyby rozszerzenie zakresu stosowania niniejszej dyrektywy, uwzględniając rozwój sytuacji w dziedzinie cyberprzestępczości. Rozwój ten mógłby obejmować wszelki rozwój technologii, np. umożliwiający skuteczniejsze egzekwowanie prawa w przypadku ataków na systemy informatyczne, względnie ułatwiający zapobieganie takim atakom lub minimalizację ich skutków. W tym celu Komisja powinna wziąć pod uwagę dostępne analizy i sprawozdania opracowywane przez właściwe podmioty, zwłaszcza przez Europol i ENISA.

(26) W celu skutecznego zwalczania cyberprzestępczości konieczne jest zwiększenie odporności systemów informatycznych przez ich lepsze zabezpieczenie przed cyberatakami, co wymaga przyjęcia odpowiednich środków. Państwa członkowskie powinny podejmować odpowiednie środki, by chronić ich krytyczną infrastrukturę przed cyberatakami; w ramach tej ochrony państwa

([1]) Dz.U. L 121 z 15.5.2009, s. 37.

członkowskie powinny rozważyć zabezpieczenie swoich systemów informatycznych i zawartych w nich danych. Zapewnianie dostatecznego poziomu ochrony i bezpieczeństwa systemów informatycznych przez osoby prawne - na przykład w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej zgodnie z obecnym ustawodawstwem Unii dotyczącym prywatności oraz łączności elektronicznej i ochrony danych - stanowi podstawową część kompleksowego podejścia do skutecznego zwalczania cyberprzestępczości. Należy zapewnić odpowiedni poziom ochrony przed racjonalnie dającymi się określić zagrożeniami i słabymi punktami zgodnie ze stanem technologii w poszczególnych sektorach oraz konkretnymi okolicznościami przetwarzania danych. Koszty i obciążenia z tytułu takiej ochrony powinny być proporcjonalne do prawdopodobnej szkody, jaką spowodowałby cyberatak. Państwa członkowskie zachęca się do zapewnienia stosownych środków w prawie krajowym, nakładających odpowiedzialność w przypadkach gdy osoba prawna wyraźnie nie zapewniła odpowiedniego poziomu ochrony przeciwko cyberatakom.

(27) Znaczące luki i różnice w przepisach państw członkowskich i ich procedurach karnych w dziedzinie ataków na systemy informatyczne mogą utrudniać walkę z przestępczością zorganizowaną i terroryzmem oraz komplikować skuteczną współpracę sądową i policyjną w tej dziedzinie. Międzynarodowy i ponadgraniczny charakter współczesnych systemów informatycznych nadaje atakom na takie systemy wymiar transgraniczny, przez co jeszcze pilniejsza staje się potrzeba dalszych działań na rzecz zbliżenia prawa karnego w tej dziedzinie. Ponadto koordynacja ścigania przypadków ataków na systemy informatyczne powinna zostać ułatwiona dzięki odpowiedniemu wdrożeniu i stosowaniu decyzji ramowej Rady 2009/948/WSiSW z dnia 30 listopada 2009 r. w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów ([1]). Państwa członkowskie we współpracy z Unią powinny także dążyć do poprawienia międzynarodowej współpracy związanej z bezpieczeństwem systemów informatycznych, sieci komputerowych i danych komputerowych. W każdej umowie międzynarodowej dotyczącej wymiany danych powinno się należycie uwzględnić bezpieczeństwo przekazywania i przechowywania danych.

(28) Lepsza współpraca między właściwymi organami ścigania a organami sądowymi w całej Unii ma zasadnicze znaczenie dla skutecznego zwalczania cyberprzestępczości. W związku z tym należy zachęcać do intensyfikacji starań na rzecz odpowiedniego szkolenia właściwych organów, by ulepszyć ich wiedzę na temat cyberprzestępczości i jej skutków oraz by wspierać współpracę i wymianę sprawdzonych rozwiązań - na przykład za pośrednictwem wyspecjalizowanych agencji i organów Unii. Szkolenie takie powinno mieć na celu m.in. podnoszenie wiedzy na temat różnych krajowych systemów prawnych, ewentualnych problemów prawnych i technicznych napotykanych podczas dochodzeń karnych oraz podziału kompetencji między organami krajowymi.

(29) Niniejsza dyrektywa respektuje poszanowanie praw człowieka i podstawowych wolności oraz jest zgodna z zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej oraz europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, w tym z zasadami ochrony danych osobowych, poszanowania życia prywatnego, swobody wypowiedzi i informacji, prawem do rzetelnego procesu, domniemaniem niewinności i prawem do obrony, jak również zasadami legalizmu i proporcjonalności przestępstw i kar. W szczególności niniejsza dyrektywa zmierza do pełnego zagwarantowania poszanowania tych praw i zasad oraz musi być odpowiednio do tego wdrażana.

(30) Ochrona danych osobowych jest prawem podstawowym zgodnie z art. 16 ust. 1 TFUE i art. 8 Karty praw podstawowych Unii Europejskiej. Zatem wszelkie przetwarzanie danych osobowych w ramach wprowadzania w życie niniejszej dyrektywy powinno odbywać się w pełnej zgodności z odnośnym ustawodawstwem Unii dotyczącym ochrony danych.

(31) Zgodnie z art. 3 Protokołu w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, te dwa państwa członkowskie powiadomiły o chęci uczestniczenia w przyjęciu i stosowaniu niniejszej dyrektywy.

(32) Zgodnie z art. 1 i 2 Protokołu w sprawie stanowiska Danii załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie uczestniczy w przyjęciu niniejszej dyrektywy i nie jest nią związana, ani jej nie stosuje.

(33) Ponieważ cele niniejszej dyrektywy, mianowicie zagwarantowanie, by ataki na systemy informatyczne były karane we wszystkich państwach członkowskich skutecznymi, proporcjonalnymi i odstraszającymi sankcjami karnymi, oraz poprawa współpracy pomiędzy organami wymiaru sprawiedliwości i innymi właściwymi organami, a także propagowanie tej współpracy, nie mogą zostać wystarczająco osiągnięte przez państwa członkowskie, natomiast ze względu na ich rozmiary i skutki możliwe jest lepsze ich osiągnięcie na poziomie Unii, Unia może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(34) Niniejsza dyrektywa ma na celu zmianę i rozszerzenie przepisów decyzji ramowej Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne ([2]). Ponieważ proponowane zmiany są liczne i mają istotny charakter, dla precyzji należy zastąpić w całości decyzję ramową 2005/222/WSiSW w odniesieniu do państw członkowskich uczestniczących w przyjęciu niniejszej dyrektywy,

([1]) Dz.U. L 328 z 15.12.2009, s. 42

([2]) Dz.U. L 69 z 16.3.2005, s. 67.

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

Artykuł 1

Przedmiot

Niniejsza dyrektywa ustanawia minimalne normy dotyczące określania przestępstw i kar w dziedzinie ataków na systemy informatyczne. Ma ona również na celu ułatwienie zapobiegania takim przestępstwom i usprawnienie współpracy między organami sądowymi i innymi właściwymi organami.

Artykuł 2

Definicje

Do celów niniejszej dyrektywy stosuje się następujące definicje:

a) „system informatyczny" oznacza urządzenie lub grupę wzajemnie połączonych lub powiązanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, dokonuje automatycznego przetwarzania danych komputerowych, jak również danych komputerowych przechowywanych, przetwarzanych, odzyskanych lub przekazanych przez to urządzenie lub tę grupę urządzeń, w celach ich eksploatacji, użycia, ochrony lub utrzymania;

b) „dane komputerowe" oznaczają przedstawienie faktów, informacji lub pojęć w formie nadającej się do przetwarzania w systemie informatycznym, włącznie z programem umożliwiającym wykonanie funkcji przez system informatyczny;

c) „osoba prawna" oznacza podmiot mający status osoby prawnej na mocy właściwego prawa, z wyjątkiem państw lub organów publicznych działających w ramach sprawowania przez nie władzy lub publicznych organizacji międzynarodowych;

d) „bezprawnie" oznacza działanie, o którym mowa w niniejszej dyrektywie, w tym dostęp, ingerencje lub przechwycenie, na które właściciel lub inny uprawniony do systemu lub jego części nie udzielił zgody, lub które nie jest dozwolone na mocy prawa krajowego.

Artykuł 3

Niezgodny z prawem dostęp do systemów informatycznych

Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by umyślne i bezprawne uzyskiwanie dostępu do całości lub jakiejkolwiek części systemu informatycznego, było karalne jako przestępstwo w przypadku, gdy zostało ono popełnione z naruszeniem środków bezpieczeństwa, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi.

Artykuł 4

Niezgodna z prawem ingerencja w systemy

Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by umyślne i bezprawne poważne utrudnienie lub zakłócenie funkcjonowania systemu informatycznego poprzez wprowadzenie, przekazywanie, uszkadzanie, usuwanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych lub czynienie ich niedostępnymi, było karalne jako przestępstwo, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi.

Artykuł 5

Niezgodna z prawem ingerencja w dane

Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by umyślne i bezprawne usuwanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych w systemie informatycznym lub czynienie ich niedostępnymi, było karalne jako przestępstwo, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi.

Artykuł 6

Niezgodne z prawem przechwytywanie

Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by umyślne i bezprawne przechwytywanie środkami technicznymi niepublicznych przekazów danych komputerowych do, z lub w ramach systemu informatycznego, w tym emisji elektromagnetycznych z systemu informatycznego zawierającego takie dane komputerowe, było karalne jako przestępstwo, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi.

Artykuł 7

Narzędzia do popełniania przestępstw

Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by umyślne wytwarzanie, sprzedaż, dostarczanie w celu użycia, przywóz, rozpowszechnianie lub udostępnianie w inny sposób jednego z następujących narzędzi było karalne jako przestępstwo, jeżeli zostało dokonane bezprawnie i umyślnie w celu popełnienia któregokolwiek z przestępstw, o których mowa w art. 3–6, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi:

a) programu komputerowego, zaprojektowanego lub przystosowanego głównie do celu popełniania przestępstw, o których mowa w art. 3–6;

b) hasła komputerowego, kodu dostępu lub podobnych danych umożliwiających dostęp do całości lub części systemu informatycznego.

Artykuł 8

Podżeganie, pomocnictwo oraz usiłowanie

1. Państwa członkowskie zapewniają, aby podżeganie do przestępstw, o których mowa w art. 3–7, oraz pomocnictwo w tych przestępstwach było karalne jako przestępstwo.

2. Państwa członkowskie zapewniają, aby usiłowanie popełnienia przestępstw, o których mowa w art. 4 i 5, było karalne jako przestępstwo.

Artykuł 9

Sankcje

1. Państwa członkowskie przyjmują środki niezbędne do zagwarantowania, by przestępstwa, o których mowa w art. 3–8, podlegały skutecznym, proporcjonalnym i odstraszającym sankcjom karnym.

2. Państwa członkowskie przyjmują środki niezbędne do zagwarantowania, by przestępstwa, o których mowa w art. 3–7, podlegały karze w maksymalnym wymiarze nie mniejszym niż dwa lata pozbawienia wolności, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi.

3. Państwa członkowskie przyjmują środki niezbędne do zagwarantowania, by przestępstwa, o których mowa w art. 4 i 5, jeżeli zostały dokonane umyślnie, podlegały karze w maksymalnym wymiarze co najmniej trzech lat pozbawienia

wolności, w przypadku gdy działaniem przy wykorzystaniu jednego z narzędzi, o których mowa w art. 7, zaprojektowanego lub dostosowanego głównie do tego celu, dotknięta została znaczna liczba systemów informatycznych.

4. Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by przestępstwa, o których mowa w art. 4 i 5, podlegały karze w maksymalnym wymiarze co najmniej pięciu lat pozbawienia wolności, w przypadku gdy:

a) zostały popełnione w ramach organizacji przestępczej, w rozumieniu decyzji ramowej 2008/841/WSiSW, niezależnie od tego, jaki wymiar kary w niej przewidziano;

b) powodują poważne szkody; lub

c) zostały popełnione przeciwko systemowi informatycznemu o charakterze infrastruktury krytycznej.

5. Państwa członkowskie podejmują niezbędne środki, by w przypadkach gdy przestępstwa, o których mowa w art. 4 i 5, są popełniane przez niewłaściwe użytkowanie danych osobowych innej osoby w celu uzyskania zaufania osoby trzeciej, tym samym powodując szkodę dla prawowitego posiadacza tej tożsamości, można było to uznać, zgodnie z przepisami prawa krajowego, za okoliczności obciążające, o ile okoliczności te nie są już objęte zakresem innych przestępstw karalnych na mocy ustawodawstwa krajowego.

Artykuł 10

Odpowiedzialność osób prawnych

1. Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by osoby prawne mogły zostać pociągnięte do odpowiedzialności za przestępstwa, o których mowa w art. 3–8, popełnione na ich korzyść przez jakąkolwiek osobę działającą indywidualnie albo jako członek organu osoby prawnej i pełniącą funkcje kierownicze w ramach tej osoby prawnej, w oparciu o jedną z poniższych podstaw:

a) upoważnienie do reprezentowania osoby prawnej;

b) upoważnienie do podejmowania decyzji w imieniu osoby prawnej;

c) upoważnienie do sprawowania kontroli w ramach tej osoby prawnej.

2. Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by osoby prawne mogły podlegać odpowiedzialności, gdy brak nadzoru lub kontroli przez osobę, o której mowa w ust. 1, umożliwił popełnienie przez osobę jej podlegającą któregokolwiek z przestępstw, o których mowa w art. 3–8, na korzyść tej osoby prawnej.

3. Odpowiedzialność osoby prawnej na podstawie ust. 1 i 2 nie wyklucza postępowania karnego przeciw osobom fizycznym, które są sprawcami przestępstw określonych w art. 3–8, osobami podżegającymi do popełnienia tych przestępstw lub pomocnikami w tych przestępstwach.

Artykuł 11

Kary nakładane na osoby prawne

1. Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by osoba prawna pociągnięta do odpowiedzialności na mocy art. 10 ust. 1 podlegała skutecznym, proporcjonalnym i odstraszającym karom, które obejmują grzywny o charakterze karnym lub innym oraz które mogą obejmować inne kary, takie jak:

a) pozbawienie prawa do korzystania ze świadczeń publicznych lub pomocy publicznej;

b) czasowy lub stały zakaz prowadzenia działalności gospodarczej;

c) poddanie nadzorowi sądowemu;

d) likwidację sądową;

e) czasowe lub stałe zamknięcie zakładów wykorzystanych w celu popełnienia przestępstwa.

2. Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by osoba prawna pociągnięta do odpowiedzialności na mocy art. 10 ust. 2 podlegała skutecznym, proporcjonalnym i odstraszającym karom lub innym środkom.

Artykuł 12

Jurysdykcja

1. Państwa członkowskie ustanawiają swoją jurysdykcję w odniesieniu do przestępstw, o których mowa w art. 3–8, popełnionych:

a) w całości lub w części na ich terytorium; lub

b) przez jednego z jego obywateli, co najmniej w przypadkach, gdy dany czyn stanowi przestępstwo w miejscu, w którym został popełniony.

2. Ustanawiając swoją jurysdykcję zgodnie z ust. 1 lit. a), dane państwo członkowskie zapewnia, aby obejmowała ona przypadki, w których:

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 informuje Komisję, w przypadku gdy podejmie decyzję o ustanowieniu jurysdykcji w odniesieniu do jednego z przestępstw, o których mowa w art. 3–8, popełnionego poza jego terytorium, w tym również, jeżeli:

a) miejsce zwykłego pobytu sprawcy znajduje się na jego terytorium; lub

b) przestępstwo zostało popełnione na korzyść osoby prawnej mającej swą siedzibę na jego terytorium.

Artykuł 13

Wymiana informacji

1. Do celów wymiany informacji odnoszących się do przestępstw, o których mowa w art. 3–8, państwa członkowskie zapewniają istnienie funkcjonujących krajowych punktów kontaktowych i korzystają z istniejącej sieci operacyjnych punktów kontaktowych, dostępnych 24 godziny na dobę oraz przez siedem dni w tygodniu. Państwa członkowskie zapewniają również istnienie procedur, dzięki którym w przypadku pilnych wniosków o pomoc właściwy organ w ciągu ośmiu godzin od otrzymania wniosku informuje co najmniej, czy na wniosek zostanie udzielona odpowiedź, oraz wskazuje jej formę i przewidywany czas jej udzielenia.

2. Państwa członkowskie informują Komisję o swoich wyznaczonych punktach kontaktowych, o których mowa w ust. 1. Komisja przekazuje te informacje pozostałym państwom członkowskim oraz właściwym wyspecjalizowanym agencjom i organom Unii.

3. Państwa członkowskie podejmują niezbędne środki, by zagwarantować udostępnienie odpowiednich kanałów informacyjnych, w celu ułatwienia niezwłocznego zgłaszania właściwym organom krajowym przestępstw, o których mowa w art. 3-6.

Artykuł 14

Monitorowanie i statystyki

1. Państwa członkowskie zapewniają istnienie systemu umożliwiającego rejestrowanie, tworzenie i dostarczanie danych statystycznych o przestępstwach, o których mowa w art. 3–7.

2. Dane statystyczne, o których mowa w ust. 1, obejmują co najmniej istniejące dane dotyczące liczby przestępstw, o których mowa w art. 3–7, zarejestrowanych przez państwa członkowskie oraz liczbę osób oskarżonych o popełnienie przestępstw, o których mowa w art. 3–7, i skazanych za ich popełnienie.

3. Państwa członkowskie przekazują Komisji dane zgromadzone zgodnie z niniejszym artykułem. Komisja zapewnia opublikowanie ujednoliconego przeglądu tych sprawozdań statystycznych oraz przekazanie go właściwym wyspecjalizowanym agencjom i organom Unii.

Artykuł 15

Zastąpienie decyzji ramowej 2005/222/WSiSW

Niniejszym zastępuje się decyzję ramową 2005/222/WSiSW w odniesieniu do państw członkowskich uczestniczących w przyjęciu niniejszej dyrektywy, bez uszczerbku dla zobowiązań tych państw członkowskich dotyczących terminu transpozycji decyzji ramowej do prawa krajowego.

W odniesieniu do państw członkowskich uczestniczących w przyjęciu niniejszej dyrektywy odesłania do decyzji ramowej 2005/222/WSiSW traktuje się jako odesłania do niniejszej dyrektywy.

Artykuł 16

Transpozycja

1. Państwa członkowskie wprowadzają w życie przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy do dnia 4 września 2015 r.

2. Państwa członkowskie przekazują Komisji tekst przepisów dokonujących transpozycji do prawa krajowego zobowiązań nałożonych na te państwa na mocy niniejszej dyrektywy.

3. Środki przyjęte przez państwa członkowskie zawierają odesłanie do niniejszej dyrektywy lub odesłanie takie towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odesłania określane są przez państwa członkowskie.

Artykuł 17

Sprawozdawczość

Do dnia 4 września 2017 r. Komisja przedłoży Parlamentowi Europejskiemu i Radzie sprawozdanie oceniające, w jakim stopniu państwa członkowskie podjęły środki niezbędne do wykonania niniejszej dyrektywy; sprawozdaniu w razie potrzeby będą towarzyszyć wnioski ustawodawcze. Komisja uwzględnia także postępy techniczne i prawne w dziedzinie cyberprzestępczości, zwłaszcza w odniesieniu do zakresu stosowania niniejszej dyrektywy.

Artykuł 18

Wejście w życie

Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 19

Adresaci

Niniejsza dyrektywa jest skierowana do państw członkowskich zgodnie z Traktatami.

Sporządzono w Brukseli dnia 12 sierpnia 2013 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
M. SCHULZ	L. LINKEVIČIUS
Przewodniczący	*Przewodniczący*