RICHTLINIE 2013/40/EU DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 12. August 2013

über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 83 Absatz 1,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses [1],

gemäß dem ordentlichen Gesetzgebungsverfahren [2],

in Erwägung nachstehender Gründe:

(1) Die Ziele dieser Richtlinie sind die Angleichung des Strafrechts der Mitgliedstaaten im Bereich Angriffe auf Informationssysteme, indem Mindestvorschriften zur Festlegung von Straftaten und einschlägigen Strafen festgelegt werden, sowie die Verbesserung der Zusammenarbeit zwischen den zuständigen Behörden einschließlich der Polizei und anderer spezialisierter Strafverfolgungsbehörden der Mitgliedstaaten sowie der zuständigen Agenturen und Einrichtungen der Union wie Eurojust, Europol und dessen Europäisches Zentrum zur Bekämpfung der Cyberkriminalität und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA).

(2) Informationssysteme sind für die politische, gesellschaftliche und wirtschaftliche Interaktion in der Union unverzichtbar. Die Gesellschaft ist in hohem und zunehmendem Maße von solchen Systemen abhängig. Das reibungslose Funktionieren und die Sicherheit dieser Systeme in der Union sind entscheidend für die Entwicklung des Binnenmarktes und für die Entwicklung einer wettbewerbsfähigen und innovativen Wirtschaft. Zu einem wirksamen Gesamtrahmen mit Vorbeugemaßnahmen zur Flankierung der strafrechtlichen Reaktionen auf Cyberkriminalität sollte auch die Gewährleistung eines angemessenen Schutzniveaus bei Informationssystemen gehören.

(3) Angriffe auf Informationssysteme und insbesondere mit organisierter Kriminalität im Zusammenhang stehende Angriffe sind sowohl in der Union als auch weltweit eine zunehmende Bedrohung, und es wächst die Besorgnis über mögliche Terroranschläge oder politisch motivierte Angriffe auf Informationssysteme, die Teil der kritischen Infrastruktur der Mitgliedstaaten und der Union sind. Hierdurch wird das Ziel einer sichereren Informationsgesellschaft und eines Raums der Freiheit, der Sicherheit und des Rechts gefährdet, so dass Gegenmaßnahmen auf Ebene der Union sowie eine bessere Zusammenarbeit und Koordinierung auf internationaler Ebene erforderlich sind.

(4) Es gibt in der Union eine Reihe kritischer Infrastrukturen, deren Störung oder Zerstörung erhebliche grenzüberschreitende Auswirkungen hätte. Da die Fähigkeit zum Schutz kritischer Infrastrukturen in der Union verbessert werden muss, sollten die Abwehrmaßnahmen gegen Cyberangriffe durch strenge Strafen, die der Schwere derartiger Angriffe Rechnung tragen, ergänzt werden. Als kritische Infrastrukturen könnten in Mitgliedstaaten befindliche Anlagen, Systeme oder deren Teile angesehen werden, die von wesentlicher Bedeutung für die Aufrechterhaltung grundlegender gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind, wie etwa Kraftwerke, Verkehrsnetze oder staatliche Netze, und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten.

(5) Es besteht eine Tendenz zu immer gefährlicheren und häufigeren Großangriffen auf Informationssysteme, die für den Mitgliedstaat oder für bestimmte Funktionen im öffentlichen oder privaten Sektor oft unverzichtbar sein können. Diese Tendenz geht einher mit der Entwicklung immer ausgefeilterer Methoden, wie etwa der Schaffung und Verwendung von sogenannten Botnetzen, bei denen die kriminelle Handlung in verschiedenen Stufen erfolgt, wobei jede Stufe für sich eine ernsthafte Gefahr für die öffentlichen Interessen darstellen könnte. Diese Richtlinie zielt unter anderem darauf ab, Strafen hinsichtlich der Schaffung der Botnetze einzuführen, nämlich für die Einrichtung einer ferngesteuerten Kontrolle über eine bedeutende Anzahl von Computern, indem diese durch gezielte Cyberangriffe mit Schadsoftware infiziert werden. Sobald es eingerichtet ist, kann das infizierte Netz von Computern, die das Botnetz bilden, ohne Wissen der Computerbenutzer aktiviert werden, um einen breit angelegten Cyberangriff zu starten, der in der Regel erheblichen Schaden anrichten kann, wie er in dieser Richtlinie beschrieben wird. Die Mitgliedstaaten können festlegen, was gemäß ihrem nationalen Recht und ihrer nationalen Praxis als erheblicher Schaden gilt; dazu können die Störung von Systemdiensten von erheblicher öffentlicher Bedeutung oder die Verursachung größerer finanzieller Kosten oder der Verlust personenbezogener Daten oder vertraulicher Informationen gehören.

(6) Cybergroßangriffe können durch die Störung des Betriebs der Informationssysteme und der Kommunikation wie auch durch Verlust oder Veränderung vertraulicher Informationen oder anderer Daten, die von wirtschaftlicher Bedeutung sind, erheblichen wirtschaftlichen Schaden verursachen. Besonderes Augenmerk sollte darauf gerichtet werden, innovative kleine und mittlere Unternehmen für die Bedrohungen durch solche Angriffe und ihre Verwundbarkeit durch solche Angriffe zu sensibilisieren, da sie immer stärker vom ordnungsgemäßen Funktionieren und der Verfügbarkeit von Informationssystemen abhängig sind und oft nur begrenzte Mittel in die Informationssicherheit investieren können.

[1] ABl. C 218 vom 23.7.2011, S. 130.

[2] Standpunkt des Europäischen Parlaments vom 4. Juli 2013 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 22. Juli 2013.

(7) Für eine einheitliche Strategie in den Mitgliedstaaten bei der Anwendung dieser Richtlinie sind gemeinsame Definitionen in diesem Bereich wichtig.

(8) Es sollten gemeinsame Straftatbestände für den rechtswidrigen Zugang zu Informationssystemen, den rechtswidrigen Systemeingriff, den rechtswidrigen Eingriff in Daten und das rechtswidrige Abfangen von Daten festgelegt werden, wozu es einer Einigung über die Tatbestandsmerkmale bedarf.

(9) Das Abfangen umfasst unter anderem das Abhören, die Überwachung und die Kontrolle des Inhalts von Kommunikationen sowie das Ausforschen des Inhalts von Daten entweder direkt durch den Zugang zum Informationssystem und seine Benutzung oder indirekt durch die Benutzung elektronischer Abhör- oder Mithörvorrichtungen mit technischen Hilfsmitteln.

(10) Mitgliedstaaten sollten Strafen für Angriffe auf Informationssysteme vorsehen. Diese Strafen sollten wirksam, verhältnismäßig und abschreckend sein und sollten Freiheitsstrafen und/oder Geldstrafen umfassen.

(11) Diese Richtlinie sieht zumindest dann Strafen vor, wenn kein leichter Fall vorliegt. Die Mitgliedstaaten können festlegen, was gemäß ihrem einzelstaatlichen Recht und ihrer einzelstaatlichen Praxis als leichter Fall gilt. Ein Fall kann beispielsweise als leicht eingestuft werden, wenn der durch die Straftat verursachte Schaden und/oder die Gefahr für öffentliche oder private Interessen, wie etwa die Integrität eines Computersystems oder von Computerdaten oder die Integrität, die Rechte oder andere Interessen einer Person geringfügig oder so geartet ist, dass die Verhängung einer Strafe innerhalb der gesetzlichen Grenzen oder die Begründung einer strafrechtlichen Verantwortung nicht erforderlich ist.

(12) Die Identifizierung und Meldung der mit Cyberangriffen verbundenen Bedrohungen und Gefahren sowie der entsprechenden Verwundbarkeit von Informationssystemen sind maßgeblich für eine wirksame Vorbeugung gegen Cyberangriffe und eine wirksame Reaktion auf diese Angriffe sowie für die Verbesserung der Sicherheit von Informationssystemen. Die Schaffung von Anreizen für die Meldung von Sicherheitslücken könnte hierzu beitragen. Die Mitgliedstaaten sollten sich darum bemühen, die legale Aufdeckung und Meldung von Sicherheitslücken zu ermöglichen.

(13) Schwerere Strafen sollten vorgesehen werden bei Angriffen auf ein Informationssystem, die von einer kriminellen Vereinigung im Sinne des Rahmenbeschlusses 2008/841/JI des Rates vom 24. Oktober 2008 zur Bekämpfung der organisierten Kriminalität [1] verübt werden, oder bei groß angelegten Cyberangriffen, bei denen eine beträchtliche Anzahl von Informationssystemen beeinträchtigt wird einschließlich in Fällen, in denen der Angriff dazu dient, ein Botnetz zu schaffen, oder bei denen schwere Schäden verursacht werden, einschließlich in Fällen, in denen der Angriff mittels eines Botnetzes durchgeführt wird. Es ist ferner angemessen, schwerere Strafen vorzusehen, wenn ein Angriff gegen eine kritische Infrastruktur der Mitgliedstaaten oder der Union gerichtet ist.

(14) Die Einführung wirksamer Maßnahmen gegen Identitätsdiebstahl und andere identitätsbezogene Straftaten bildet eine weitere wichtige Komponente eines integrierten Ansatzes gegen die Cyberkriminalität. Das Erfordernis von Maßnahmen der Union gegen diese Art kriminellen Verhaltens könnte auch im Rahmen der Bewertung der Frage geprüft werden, ob es eines umfassenden horizontalen Instruments der Union bedarf.

(15) In den Schlussfolgerungen des Rates vom 27. und 28. November 2008 wurde die Ausarbeitung einer neuen Strategie in Zusammenarbeit mit den Mitgliedstaaten und der Kommission angekündigt, in die auch das Übereinkommen des Europarats über Computerkriminalität aus dem Jahr 2001 einfließen soll. Dieses Übereinkommen ist der rechtliche Bezugsrahmen für die Bekämpfung der Cyberkriminalität und damit auch der Angriffe auf Informationssysteme. Die vorliegende Richtlinie baut auf dem Übereinkommen auf. Eine möglichst baldige Ratifizierung dieses Übereinkommens durch alle Mitgliedstaaten sollte als Priorität betrachtet werden.

(16) Angesichts der unterschiedlichen Art und Weise, wie Cyberangriffe ausgeführt werden können, und der raschen Entwicklung bei der Hard- und Software bezieht sich diese Richtlinie auf „Instrumente", die zur Begehung der in dieser Richtlinie vorgesehenen Straftaten verwendet werden können. Bei solchen Instrumenten kann es sich beispielsweise um Schadsoftware einschließlich jener handeln, mit der Botnetze geschaffen werden können, die für Cyberangriffe verwendet werden. Auch wenn ein Instrument für die Durchführung der in dieser Richtlinie aufgeführten Straftaten geeignet oder besonders geeignet ist, so ist es doch möglich, dass es für rechtmäßige Zwecke hergestellt worden ist. Da eine Kriminalisierung in den Fällen vermieden werden muss, in denen diese Instrumente für rechtmäßige Zwecke — wie beispielsweise Prüfung der Zuverlässigkeit von Produkten der Informationstechnologie oder der Sicherheit von Informationssystemen — hergestellt und in Verkehr gebracht worden sind, muss neben dem allgemeinen Vorsatz der direkte Vorsatz gegeben sein, diese Instrumente für das Begehen von in der Richtlinie vorgesehenen Straftaten zu verwenden.

(17) Mit dieser Richtlinie wird keine strafrechtliche Verantwortung in Fällen begründet, in denen die objektiven Tatbestandsmerkmale der in dieser Richtlinie vorgesehenen Straftaten zwar gegeben sind, die Taten aber ohne strafrechtlichen Vorsatz begangen werden, wie etwa in den Fällen, in denen eine Person nicht weiß, dass sie keine Zugangsbefugnis hatte, beispielsweise bei in Auftrag gegebenen Tests von Informationssystemen oder bei deren Schutz, wenn beispielsweise eine Person von einem Unternehmen oder Verkäufer beauftragt wird, die Stärke des Sicherheitssystems eines Informationssystems zu testen. Im Rahmen dieser Richtlinie sollten vertragliche Verpflichtungen oder Vereinbarungen zur Beschränkung des Zugangs zu Informationssystemen durch Benutzerverwaltungsrichtlinien oder Dienstleistungsbedingungen sowie arbeitsrechtliche Streitigkeiten in Bezug auf den Zugang zu Informationssystemen eines Arbeitgebers und deren Nutzung für private Zwecke keine strafrechtliche Haftung begründen, wenn ein Zugang unter diesen Umständen als unberechtigter Zugang gelten und damit die einzige Grundlage für die Strafverfolgung bilden würde. Diese Richtlinie berührt nicht das im nationalen Recht und im Recht der Union verankerte Recht auf den Zugang zu Informationen, dient aber auch nicht als Rechtfertigung eines rechtswidrigen oder eigenmächtigen Zugangs.

[1] ABl. L 300 vom 11.11.2008, S. 42.

(18) Cyberangriffe könnten durch verschiedene Umstände erleichtert werden, so etwa, wenn der Täter im Rahmen seines Beschäftigungsverhältnisses über einen Zugang zu in den betroffenen Informationssystemen vorhandenen Sicherheitssystemen verfügt. Im Rahmen des nationalen Rechts sollten solche Umstände in Strafverfahren angemessen berücksichtigt werden.

(19) Die Mitgliedstaaten sollten in ihren innerstaatlichen Rechtsvorschriften eine Regelung für erschwerende Umstände — im Einklang mit den in ihrem Rechtssystem geltenden einschlägigen Bestimmungen — vorsehen. Sie sollten sicherstellen, dass die Richter diese bei der Verurteilung von Straftätern berücksichtigen können. Es liegt im Ermessen des Richters, diese Umstände zusammen mit den übrigen Sachumständen des jeweiligen Falles zu bewerten.

(20) Diese Richtlinie enthält keine Bestimmungen über die Voraussetzungen dafür, dass die Gerichtsbarkeit über die in dieser Richtlinie genannten Straftaten ausgeübt werden kann, wie etwa eine am Tatort erstattete Anzeige des Opfers, eine Anzeige des Staates, in dem sich der Tatort befindet, oder die Tatsache, dass der Täter am Tatort nicht verfolgt wurde.

(21) Im Rahmen dieser Richtlinie sind Staaten und öffentliche Stellen nach wie vor in vollem Umfang dazu verpflichtet, die Achtung der Menschenrechte und Grundfreiheiten im Einklang mit den bestehenden internationalen Verpflichtungen zu gewährleisten.

(22) Diese Richtlinie stärkt die Rolle von Netzwerken wie des G8-Netzes oder des Netzes der Kontaktstellen des Europarats, die an sieben Wochentagen 24 Stunden täglich für den Informationsaustausch zur Verfügung stehen. Diese Kontaktstellen sollten in der Lage sein, wirksame Hilfe zu leisten und damit beispielsweise den Austausch verfügbarer einschlägiger Informationen und die Bereitstellung technischer Beratung oder rechtlicher Informationen für Ermittlungen und Verfahren wegen Straftaten im Zusammenhang mit Informationssystemen und dazugehörigen Daten, die den ersuchenden Mitgliedstaat betreffen, zu erleichtern. Um den reibungslosen Betrieb der Netze sicherzustellen, sollte jede Kontaktstelle in der Lage sein, beschleunigt — unter anderem mithilfe geschulten und entsprechend ausgerüsteten Personals — mit der Kontaktstelle eines anderen Mitgliedstaats Kontakt aufzunehmen. Angesichts der Schnelligkeit, mit der Cyber-Großangriffe ausgeführt werden können, sollten die Mitgliedstaaten in der Lage sein, umgehend auf dringende Ersuchen dieser Kontaktstellen um Unterstützung zu reagieren. In diesen Fällen kann es zweckmäßig sein, dass neben dem Informationsersuchen auch telefonisch Kontakt aufgenommen wird, um dafür zu sorgen, dass der ersuchte Mitgliedstaat das Ersuchen zügig bearbeitet und dass innerhalb von acht Stunden eine Rückmeldung erfolgt.

(23) Um Angriffe auf Informationssysteme zu verhindern und zu bekämpfen, ist die Zusammenarbeit zwischen Behörden einerseits und der Privatwirtschaft und Zivilgesellschaft andererseits sehr wichtig. Die Zusammenarbeit zwischen Diensteanbietern, Herstellern sowie Strafverfolgungsstellen und Justizbehörden muss gefördert und verbessert werden, wobei jedoch die Rechtsstaatlichkeit uneingeschränkt zu achten ist. Eine solche Zusammenarbeit könnte die Unterstützung von Diensteanbietern bei der Sicherstellung potenzieller Beweismittel, bei der Bereitstellung von Anhaltspunkten zur Ermittlung von Tätern und — als letztes Mittel — bei der vollständigen oder teilweisen Abschaltung von beeinträchtigten oder für unrechtmäßige Zwecke verwendeten Informationssystemen oder Funktionen nach Maßgabe des nationalen Rechts und der nationalen Gepflogenheiten umfassen. Die Mitgliedstaaten sollten ferner in Betracht ziehen, für den Informationsaustausch in Bezug auf die in den Anwendungsbereich dieser Richtlinie fallenden Straftaten Netze für die Zusammenarbeit und Partnerschaft mit Diensteanbietern und Herstellern einzurichten.

(24) Es ist erforderlich, vergleichbare Daten in Bezug auf die in dieser Richtlinie vorgesehenen Straftaten zu erheben. Die betreffenden Daten sollten den zuständigen spezialisierten Agenturen und Einrichtungen der Union wie Europol und der ENISA im Einklang mit ihren Aufgaben und ihrem Informationsbedarf zur Verfügung gestellt werden, damit ein umfassenderes Bild des Problems der Cyberkriminalität und der Netz- und Informationssicherheit auf Unionsebene gewonnen und somit ein Beitrag zur Ausarbeitung wirksamerer Abhilfemaßnahmen geleistet werden kann. Die Mitgliedstaaten sollten Europol und dessen Europäischem Zentrum zur Bekämpfung der Cyberkriminalität Informationen über die Vorgehensweisen der Täter zur Verfügung stellen, damit die Bewertungen der Bedrohungslage und strategischen Analysen zur Cyberkriminalität gemäß dem Beschluss 2009/371/JI des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol) ([1]) durchgeführt werden können. Die Bereitstellung von Informationen kann ein besseres Verständnis gegenwärtiger und zukünftiger Bedrohungen erleichtern und damit zu einer angemesseneren und zielorientierten Beschlussfassung über Bekämpfung und Verhütung von Angriffen auf Informationssysteme beitragen.

(25) Die Kommission sollte einen Bericht über die Anwendung der Richtlinie vorlegen und erforderliche Gesetzgebungsvorschläge unterbreiten, die unter Berücksichtigung der Entwicklungen in Bezug auf die Cyberkriminalität zu einer Erweiterung des Anwendungsbereichs dieser Richtlinie führen könnten. Solche künftigen Entwicklungen könnten technologische Entwicklungen umfassen, die beispielsweise eine wirksamere Strafverfolgung bei Angriffen auf Informationssysteme ermöglichen oder der Verhütung solcher Angriffe oder der Minimierung ihrer Auswirkungen dienen. Zu diesem Zweck sollte die Kommission die verfügbaren Analysen und Berichte berücksichtigen, die von den einschlägigen Akteuren und insbesondere von Europol und ENISA ausgearbeitet worden sind.

(26) Um die Cyberkriminalität wirksam zu bekämpfen, ist es erforderlich, die Widerstandsfähigkeit von Informationssystemen dadurch zu erhöhen, dass geeignete Maßnahmen ergriffen werden, um sie wirksamer gegen Cyberangriffe zu schützen. Die Mitgliedstaaten sollten die erforderlichen Maßnahmen treffen, um die Informationssysteme, die Teil ihrer kritischen Infrastruktur sind, vor Cyberangriffen zu schützen, und in diesem Rahmen auch prüfen, wie ihre Informationssysteme und die dazugehörigen Daten zu schützen sind. Eine wesentliche Komponente eines umfassenden Konzepts zur wirksamen Bekämpfung der Cyberkriminalität besteht darin, dass ein

([1]) ABl. L 121 vom 15.5.2009, S. 37.

angemessenes Schutz- und Sicherheitsniveau bei Informationssystemen durch juristische Personen — beispielsweise in Verbindung mit der Bereitstellung öffentlich zugänglicher Kommunikationsdienste im Einklang mit den bestehenden Unionsvorschriften über den Schutz der Privatsphäre und elektronische Kommunikation sowie Datenschutz — gewährleistet wird. Gegen Bedrohungen und Schwachstellen, die ohne übermäßigen Aufwand erkennbar sind, sollten ein angemessenes Schutzniveau gemäß dem neuesten Stand der Technik für spezifische Branchen und spezifische Situationen der Datenverarbeitung geboten werden. Die Kosten und der Aufwand eines solchen Schutzes sollten in einem angemessenen Verhältnis zu dem Schaden stehen, der bei einem Cyberangriff für die Betroffenen zu erwarten wäre. Die Mitgliedstaaten werden ermutigt, für die einschlägigen Maßnahmen zur Begründung einer Haftung im Rahmen ihres nationalen Rechts in den Fällen zu sorgen, in denen eine juristische Person eindeutig kein ausreichendes Niveau des Schutzes vor Cyberangriffen gewährleistet hat.

(27) Größere Abweichungen und Diskrepanzen zwischen den Rechtsvorschriften und Strafverfahren der Mitgliedstaaten im Bereich von Angriffen auf Informationssysteme können die Bekämpfung der organisierten Kriminalität und des Terrorismus behindern und unter Umständen eine wirksame polizeiliche und justizielle Zusammenarbeit bei der Abwehr von Angriffen auf Informationssysteme erschweren. Der länder- und grenzübergreifende Charakter moderner Informationssysteme bedeutet, dass auch Angriffe auf solche Systeme eine grenzüberschreitende Dimension annehmen, was den dringenden Bedarf an weiteren Maßnahmen zur Angleichung des Strafrechts in diesem Bereich unterstreicht. Die Koordinierung der Strafverfolgung bei Angriffen auf Informationssysteme sollte mithilfe einer angemessenen Umsetzung und Anwendung des Rahmenbeschlusses 2009/948/JI des Rates vom 30. November 2009 zur Vermeidung und Beilegung von Kompetenzkonflikten in Strafverfahren [1] erleichtert werden. Die Mitgliedstaaten sollten sich in Zusammenarbeit mit der Union ferner um die Verbesserung der internationalen Zusammenarbeit in Bezug auf die Sicherheit von Informationssystemen, Computernetzen und Computerdaten bemühen. Der Sicherheit der Datenübertragung und -speicherung sollte bei allen internationalen Übereinkünften, bei denen der Austausch von Daten eine Rolle spielt, angemessen Rechnung getragen werden.

(28) Eine verbesserte Zusammenarbeit zwischen den zuständigen Strafverfolgungsstellen und Justizbehörden in der gesamten Union ist für die wirksame Bekämpfung der Cyberkriminalität von wesentlicher Bedeutung. In diesem Zusammenhang sollte die Intensivierung der Bemühungen um eine angemessene Schulung der einschlägigen Behörden im Hinblick auf ein besseres Verständnis der Cyberkriminalität und ihrer Auswirkungen und die Verstärkung der Zusammenarbeit und des Austauschs bewährter Verfahren beispielsweise über die zuständigen spezialisierten Agenturen und Einrichtungen der Union gefördert werden. Mit der betreffenden Schulung sollte unter anderem angestrebt werden, eine verstärkte Sensibilisierung hinsichtlich der unterschiedlichen nationalen Rechtssysteme, der möglichen rechtlichen und technischen Probleme bei strafrechtlichen Ermittlungen und der Aufteilung der Zuständigkeiten zwischen den einschlägigen nationalen Behörden zu bewirken.

(29) Diese Richtlinie achtet die Menschenrechte und Grundfreiheiten und wahrt die Grundsätze, die insbesondere mit der Charta der Grundrechte der Europäischen Union und der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten anerkannt wurden, namentlich der Schutz personenbezogener Daten, das Recht auf Schutz der Privatsphäre, die Meinungs- und Informationsfreiheit, das Recht auf ein faires Verfahren, die Unschuldsvermutung und die Gewährleistung der Verteidigungsrechte sowie das Gesetzlichkeits- und Verhältnismäßigkeitsprinzip in Bezug auf Straftaten und Strafen. Diese Richtlinie, mit der die uneingeschränkte Wahrung dieser Rechte und Grundsätze gewährleistet werden soll, ist entsprechend umzusetzen.

(30) Der Schutz personenbezogener Daten ist ein Grundrecht gemäß Artikel 16 Absatz 1 AEUV und Artikel 8 der Charta der Grundrechte der Europäischen Union. Daher sollte jede Verarbeitung von Daten im Rahmen der Umsetzung dieser Richtlinie uneingeschränkt dem einschlägigen Unionsrecht über Datenschutz entsprechen.

(31) Gemäß Artikel 3 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts haben diese Mitgliedstaaten mitgeteilt, dass sie sich an der Annahme und Anwendung dieser Richtlinie beteiligen möchten.

(32) Nach den Artikeln 1 und 2 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls über die Position Dänemarks beteiligt sich Dänemark nicht an der Annahme dieser Richtlinie und ist weder durch diese Richtlinie gebunden noch zu ihrer Anwendung verpflichtet.

(33) Da die Ziele dieser Richtlinie, nämlich Angriffe auf Informationssysteme in allen Mitgliedstaaten mit wirksamen, verhältnismäßigen und abschreckenden Strafen zu ahnden und die justizielle Zusammenarbeit zu verbessern und zu fördern, auf Ebene der Mitgliedstaaten nicht ausreichend verwirklicht werden können, und daher aufgrund ihres Ausmaßes oder ihrer Wirkung besser auf Unionsebene zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union niedergelegten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Richtlinie nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus.

(34) Mit dieser Richtlinie sollen die Bestimmungen des Rahmenbeschlusses 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme [2] geändert und ausgeweitet werden. Da die vorzunehmenden Änderungen sowohl bezüglich der Zahl als auch hinsichtlich des Inhalts erheblich sind, sollte der Rahmenbeschluss 2005/222/JI aus Gründen der Klarheit für die sich an der Annahme dieser Richtlinie beteiligenden Mitgliedstaaten vollständig ersetzt werden —

[1] ABl. L 328 vom 15.12.2009, S. 42.

[2] ABl. L 69 vom 16.3.2005, S. 67.

HABEN FOLGENDE RICHTLINIE ERLASSEN:

Artikel 1

Gegenstand

Mit dieser Richtlinie werden Mindestvorschriften zur Festlegung von Straftaten und Strafen bei Angriffen auf Informationssysteme festgelegt. Diese Richtlinie soll überdies die Verhinderung derartiger Straftaten erleichtern und die Zusammenarbeit zwischen Justizbehörden und anderen zuständigen Behörden verbessern.

Artikel 2

Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

a) „Informationssystem" eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung von Computerdaten durchführen, sowie die von ihr oder ihnen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten, abgerufenen oder übertragenen Computerdaten;

b) „Computerdaten" jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Informationssystem geeigneten Form, einschließlich eines Programms, das die Ausführung einer Funktion durch ein Informationssystem auslösen kann;

c) „juristische Person" jedes Rechtssubjekt, das den Status der juristischen Person nach dem anwendbaren Recht besitzt, mit Ausnahme von Staaten oder anderen Körperschaften des öffentlichen Rechts in der Ausübung hoheitlicher Rechte und von öffentlich-rechtlichen internationalen Organisationen;

d) „unbefugt" ein in dieser Richtlinie genanntes Verhalten, einschließlich Zugang, Eingriff oder Abfangen, das vom Eigentümer oder einem anderen Rechtsinhaber des Systems oder eines Teils des Systems nicht gestattet wurde oder das nach den einzelstaatlichen Rechtsvorschriften nicht zulässig ist.

Artikel 3

Rechtswidriger Zugang zu Informationssystemen

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass der vorsätzliche unbefugte Zugang zu einem Informationssystem als Ganzem oder zu einem Teil davon, wenn dieser Zugang durch eine Verletzung von Sicherheitsmaßnahmen erfolgt, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

Artikel 4

Rechtswidriger Systemeingriff

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass die vorsätzliche und unbefugte schwere Behinderung oder Störung des Betriebs eines Informationssystems durch Eingeben von Computerdaten, durch Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern und Unterdrücken von Computerdaten und durch Unzugänglichmachen von Computerdaten zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

Artikel 5

Rechtswidriger Eingriff in Daten

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche und unbefugte Löschen, Beschädigen, Beeinträchtigen, Verändern, Unterdrücken von Computerdaten eines Informationssystems und das Unzugänglichmachen solcher Daten zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

Artikel 6

Rechtswidriges Abfangen von Daten

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche und unbefugte, mit technischen Hilfsmitteln bewirkte Abfangen nichtöffentlicher Computerdatenübermittlungen an ein Informationssystem, aus einem Informationssystem oder innerhalb eines Informationssystems einschließlich elektromagnetischer Abstrahlungen aus einem Informationssystem, das Träger solcher Computerdaten ist, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

Artikel 7

Tatwerkzeuge

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche und unbefugte Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen folgender Instrumente, das mit der Absicht erfolgt, eine Straftat im Sinne der Artikel 3 bis 6 zu begehen, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt:

a) eines Computerprogramms, das in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine Straftat im Sinne der Artikel 3 bis 6 zu begehen;

b) eines Computerpassworts, eines Zugangscodes oder ähnlicher Daten, die den Zugang zu einem Informationssystem als Ganzem oder zu einem Teil davon ermöglichen.

Artikel 8

Anstiftung, Beihilfe und Versuch

(1) Die Mitgliedstaaten stellen sicher, dass die Anstiftung oder Beihilfe zur Begehung einer Straftat im Sinne der Artikel 3 bis 7 unter Strafe gestellt wird.

(2) Die Mitgliedstaaten stellen sicher, dass der Versuch der Begehung einer Straftat im Sinne der Artikel 4 und 5 unter Strafe gestellt wird.

Artikel 9

Strafen

(1) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass die Straftaten im Sinne der Artikel 3 bis 8 mit wirksamen, angemessenen und abschreckenden Strafen geahndet werden.

(2) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass Straftaten im Sinne der Artikel 3 bis 7 zumindest dann mit Freiheitsstrafen im Höchstmaß von mindestens zwei Jahren geahndet werden, wenn kein leichter Fall vorliegt.

(3) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass die Straftaten im Sinne der Artikel 4 und 5 mit Freiheitsstrafen im Höchstmaß von

mindestens drei Jahren geahndet werden, wenn sie vorsätzlich begangen werden und eine beträchtliche Anzahl von Informationssystemen unter Verwendung eines in Artikel 7 genannten Instruments, das in erster Linie dafür ausgerichtet oder hergerichtet wurde, beeinträchtigt wird.

(4) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass Straftaten im Sinne der Artikel 4 und 5 mit Freiheitsstrafen im Höchstmaß von mindestens fünf Jahren geahndet werden, wenn

a) sie im Rahmen einer kriminellen Vereinigung im Sinne des Rahmenbeschlusses 2008/841/JI ungeachtet der dort genannten Strafen begangen wurden;

b) sie einen schweren Schaden verursachen oder

c) sie gegen ein Informationssystem einer kritischen Infrastruktur verübt wurden.

(5) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass der Missbrauch der personenbezogenen Daten einer anderen Person mit dem Ziel, das Vertrauen eines Dritten zu gewinnen, wodurch dem rechtmäßigen Identitätseigentümer ein Schaden zugefügt wird, im Einklang mit dem nationalen Recht als erschwerender Umstand bei der Begehung von Straftaten nach den Artikeln 4 und 5 eingestuft werden kann, soweit der betreffende Umstand nicht bereits eine andere Straftat im Sinne des nationalen Rechts darstellt.

Artikel 10

Verantwortlichkeit juristischer Personen

(1) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass eine juristische Person für eine Straftat im Sinne der Artikel 3 bis 8 verantwortlich gemacht werden kann, die zu ihren Gunsten von einer Person begangen wurde, die entweder allein oder als Teil eines Organs der juristischen Person gehandelt hat und die eine Führungsposition innerhalb der juristischen Person innehat, aufgrund

a) einer Befugnis zur Vertretung der juristischen Person,

b) einer Befugnis, Entscheidungen im Namen der juristischen Person zu treffen oder

c) einer Kontrollbefugnis innerhalb der juristischen Person.

(2) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass eine juristische Person verantwortlich gemacht werden kann, wenn mangelnde Überwachung oder Kontrolle seitens einer in Absatz 1 genannten Person die Begehung einer Straftat nach den Artikeln 3 bis 8 zugunsten der juristischen Person durch eine ihr unterstellte Person ermöglicht hat.

(3) Die Verantwortlichkeit der juristischen Personen nach den Absätzen 1 und 2 schließt die strafrechtliche Verfolgung natürlicher Personen als Täter, Anstifter oder Gehilfen bei einer Straftat im Sinne der Artikel 3 bis 8 nicht aus.

Artikel 11

Sanktionen gegen juristische Personen

(1) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass gegen eine im Sinne von Artikel 10 Absatz 1 verantwortliche juristische Person wirksame, verhältnismäßige und abschreckende Sanktionen verhängt werden können, zu denen Geldstrafen oder Geldbußen gehören und zu denen andere Sanktionen gehören können wie etwa:

a) Ausschluss von öffentlichen Zuwendungen oder Hilfen,

b) vorübergehendes oder ständiges Verbot der Ausübung einer Handelstätigkeit,

c) richterliche Aufsicht,

d) richterlich angeordnete Eröffnung des Liquidationsverfahrens oder

e) vorübergehende oder endgültige Schließung von Einrichtungen, die zur Begehung der Straftat genutzt wurden.

(2) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass gegen eine im Sinne von Artikel 10 Absatz 2 verantwortliche juristische Person wirksame, angemessene und abschreckende Sanktionen oder andere Maßnahmen verhängt werden können.

Artikel 12

Gerichtliche Zuständigkeit

(1) Jeder Mitgliedstaat begründet seine Zuständigkeit für die in den Artikeln 3 bis 8 genannten Straftaten, wenn diese

a) ganz oder teilweise in seinem Hoheitsgebiet oder

b) von einem seiner Staatsangehörigen begangen wurden, zumindest in den Fällen, in denen die Tat an dem Ort, an dem sie begangen wurde, eine Straftat darstellt.

(2) Bei der Begründung seiner Zuständigkeit gemäß Absatz 1 Buchstabe a stellt jeder Mitgliedstaat sicher, dass sich seine Zuständigkeit auch auf Fälle erstreckt, in denen

a) sich der Täter bei der Begehung der Straftat physisch in seinem Hoheitsgebiet aufhält, unabhängig davon, ob sich die Straftat gegen ein Informationssystem innerhalb oder außerhalb seines Hoheitsgebiets richtet, oder

b) sich die Straftat gegen ein Informationssystem in seinem Hoheitsgebiet richtet, unabhängig davon, ob sich der Täter bei der Begehung der Straftat physisch im Hoheitsgebiet dieses Mitgliedstaats aufhält.

(3) Ein Mitgliedstaat unterrichtet die Kommission über seine Entscheidung, eine gerichtliche Zuständigkeit für Straftaten nach den Artikeln 3 bis 8, die außerhalb seines Hoheitsgebiets begangen wurden, zu begründen, einschließlich in Fällen, in denen

a) der gewöhnliche Aufenthalt des Straftäters in seinem Hoheitsgebiet liegt oder

b) die Straftat zugunsten einer in seinem Hoheitsgebiet niedergelassenen juristischen Person begangen wird.

Artikel 13

Informationsaustausch

(1) Zum Zweck des Informationsaustauschs über Straftaten nach den Artikeln 3 bis 8 stellen die Mitgliedstaaten sicher, dass sie über eine operative nationale Kontaktstelle verfügen, und das bestehende Netz der operativen Kontaktstellen, die an sieben Wochentagen 24 Stunden täglich zur Verfügung stehen, nutzen. Die Mitgliedstaaten sorgen ferner dafür, dass Verfahren vorhanden sind, mit denen die zuständige Behörde bei dringenden Ersuchen um Unterstützung binnen höchstens acht Stunden nach Eingang des Ersuchens zumindest mitteilen können, ob das Ersuchen beantwortet wird und in welcher Form und wann dies voraussichtlich erfolgen wird.

(2) Die Mitgliedstaaten teilen der Kommission ihre in Absatz 1 genannte Kontaktstelle mit. Die Kommission leitet diese Informationen an die anderen Mitgliedstaaten und die spezialisierten Agenturen und Einrichtungen der Union weiter.

(3) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass geeignete Meldekanäle zur Verfügung stehen, damit die Meldung der in den Artikeln 3 bis 6 aufgeführten Straftaten an die zuständigen nationalen Behörden unverzüglich erfolgen kann.

Artikel 14

Kontrolle und Statistiken

(1) Die Mitgliedstaaten sorgen dafür, dass ein System für die Aufzeichnung, Erstellung und Bereitstellung statistischer Daten zu den Straftaten im Sinne der Artikel 3 bis 7 bereitsteht.

(2) Die statistischen Daten gemäß Absatz 1 umfassen zumindest die vorhandenen Daten über die Anzahl der in den Mitgliedstaaten erfassten Straftaten im Sinne der Artikel 3 bis 7 und die Anzahl der Personen, die wegen einer Straftat im Sinne der Artikel 3 bis 7 verfolgt und verurteilt worden sind.

(3) Die Mitgliedstaaten übermitteln der Kommission die nach Maßgabe dieses Artikels erfassten Daten. Die Kommission sorgt dafür, dass eine konsolidierte Zusammenfassung dieser statistischen Berichte veröffentlicht und den spezialisierten Agenturen und Einrichtungen der Union zugeleitet wird.

Artikel 15

Ersetzung des Rahmenbeschlusses 2005/222/JI

Der Rahmenbeschluss 2005/222/JI wird in Bezug auf die Mitgliedstaaten ersetzt, die sich an der Annahme dieser Richtlinie beteiligen, unbeschadet der Pflichten der Mitgliedstaaten im Zusammenhang mit den Fristen für die Umsetzung des Rahmenbeschlusses in innerstaatliches Recht.

In Bezug auf die Mitgliedstaaten, die sich an der Annahme dieser Richtlinie beteiligen, gelten Verweise auf den Rahmenbeschluss 2005/222/JI als Verweise auf die vorliegende Richtlinie.

Artikel 16

Umsetzung

(1) Die Mitgliedstaaten setzen die erforderlichen Rechts- und Verwaltungsvorschriften in Kraft, um dieser Richtlinie bis zum 4. September 2015 nachzukommen.

(2) Die Mitgliedstaaten übermitteln der Kommission den Wortlaut der innerstaatlichen Maßnahmen zur Umsetzung ihrer Verpflichtungen aus dieser Richtlinie.

(3) Bei Erlass dieser Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten dieser Bezugnahme.

Artikel 17

Berichterstattung

Die Kommission legt dem Europäischen Parlament und dem Rat bis zum 4. September 2017 einen Bericht darüber vor, inwieweit die Mitgliedstaaten die zur Einhaltung dieser Richtlinie erforderlichen Maßnahmen ergriffen haben, und unterbreitet erforderlichenfalls Gesetzgebungsvorschläge. Die Kommission berücksichtigt auch die technischen und rechtlichen Entwicklungen im Bereich der Cyberkriminalität, insbesondere hinsichtlich des Anwendungsbereichs dieser Richtlinie.

Artikel 18

Inkrafttreten

Diese Richtlinie tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Artikel 19

Adressaten

Diese Richtlinie ist gemäß den Verträgen an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am 12. August 2013.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*
M. SCHULZ	L. LINKEVIČIUS